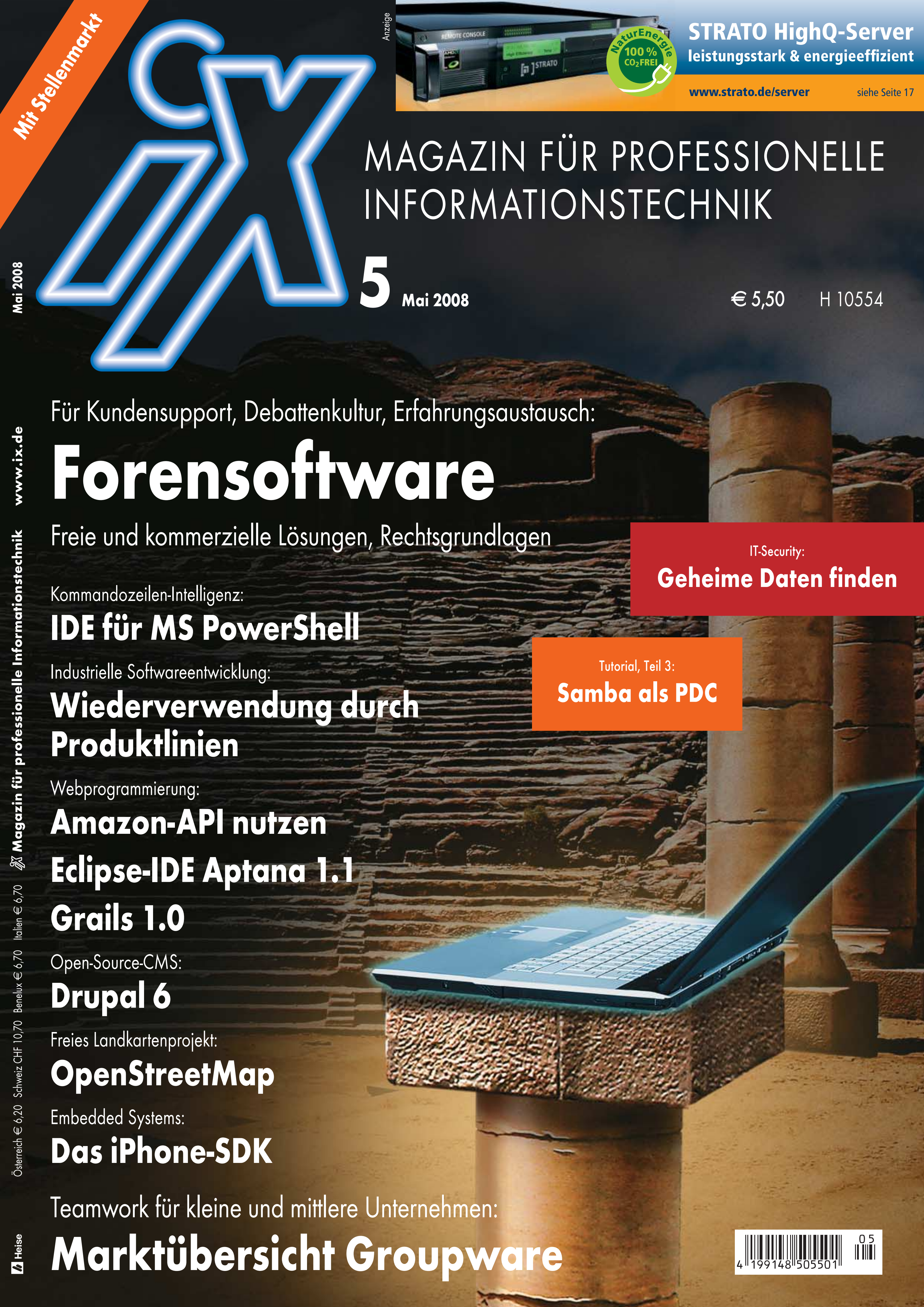

Mit Stellenmarkt
iX
Anzeige
STRATO HighQ-Server
leistungsstark & energieeffizient
www.strato.de/server
siehe Seite 17
MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK
5 Mai 2008
€ 5,50
H 10554
Für Kundensupport, Debattenkultur, Erfahrungsaustausch:
Forensoftware
Freie und kommerzielle Lösungen, Rechtsgrundlagen
IT-Security:
Geheime Daten finden
Kommandozeilen-Intelligenz:
IDE für MS PowerShell
Tutorial, Teil 3:
Samba als PDC
Industrielle Softwareentwicklung:
Wiederverwendung durch Produktlinien
Webprogrammierung:
Amazon-API nutzen
Eclipse-IDE Aptana 1.1
Grails 1.0
Open-Source-CMS:
Drupal 6
Freies Landkartenprojekt:
OpenStreetMap
Embedded Systems:
Das iPhone-SDK
Teamwork für kleine und mittlere Unternehmen:
Marktübersicht Groupware
Heise
Österreich € 6,20 Schweiz CHF 10,70 Benelux € 6,70 Italien € 6,70
iX Magazin für professionelle Informationstechnik www.ix.de
Mai 2008
4 199148 505501 05

Neulich im Büro

Offen ist gut. Abgesegnete Offenheit ist besser, optimal allseits akzeptierte Absegnung. Den zweiten Status hat Microsofts Spezifikation des Office Open XML (OOXML) Anfang April erreicht, indem die International Organization for Standardization und die International Electrotechnical Commission sie in den Rang eines ISO/IEC-Standards erhoben (siehe Seite 31). DIS 29500 heißt das jüngste Kind aus deren Dokumenten-Portfolio, zu dem auch der schon Anfang Mai 2006 von der ISO geadelte OOXML-Konkurrent Open Document Format (ODF) und zwei PDF-Spezifikationen gehören.

Eine weitere Standardisierungsinstitution, Ecma International, hatte das Format für Büroanwendungen bei der ISO eingereicht, nachdem sie selbst im Dezember 2006 OOXML als ihren Standard 376 verabschiedet hatte. Bei der ISO können nationale Gremien innerhalb von zwei Monaten noch formale Bedenken erheben.

iX-Links bringt der Mai

Beginnend mit dieser Ausgabe erhalten die Artikel, die Verweise ins Web enthalten, am Ende einen Hinweis darauf, dass diese Webadressen auf dem Server der *iX* abrufbar sind. Über ein rechts oben auf der *iX*-Homepage angesiedeltes Eingabefeld kommt man umgehend zu den Links. In diesem Heft gilt das leider noch nicht für viele Artikel. Trotzdem schon viel Spaß …

Dass es während des sich hinziehenden Prozedere teilweise seltsam zuging, wie unter anderem Proteste in Norwegen annehmen lassen, dürfte für diejenigen, die Software-Entscheidungen zu treffen haben, in zwei Jahren von ungefähr so großem Interesse sein wie ein unberechtigter, aber vielleicht entscheidender Elfmeter in der 90. Minute, der die Meisterschaft kostet beziehungsweise bringt. Wichtiger könnte sein, dass die Anerkennung nicht bedeutet, dass die EU in ihren Anti-Trust-Bemühungen zwangsläufig innehält oder gar mit ihnen aufhört.

Was für Microsoft bleibt, ist außer dem symbolischen (und politischen) Erfolg, die eigenen Dateiformate von der ISO standardisiert bekommen zu haben[1], vor allem die Aussicht, sich nun nicht mehr als proprietär beschimpfen lassen zu müssen. Firmen-CTOs und Behördenleiter, die seit Jahren mit Microsofts Produkten arbeiten, müssen angesichts von Forderungen nach offener Software jetzt nicht mehr befürchten, auf ODF umschwenken zu müssen, weil es das einzige offene Format für Büroanwendungen ist. Sie können schlicht auf die ISO-Entscheidung verweisen.

Als letztes der Designziele für XML hatten die Herausgeber der Spezifikation seinerzeit vermerkt: „Terseness in XML markup is of minimal importance.“ Mindestens an diese Losung haben sich die Redmonder bei OOXML gehalten, denn 6000 Seiten Spezifikation dürfte niemand knapp (engl.: terse) nennen wollen, und sie schreien förmlich danach, nicht vollständig implementiert zu werden. Das wiederum könnte sich als Haupthindernis für die vielbeschworene Interoperabilität erweisen, denn wenn selbst Microsoft nicht alle Aspekte der 6000 Seiten implementieren kann oder will, gibt es keine Gewissheit für alle anderen, dass ihre Auswahl sich mit der des großen Office-Herstellers deckt.

Vielleicht erarbeiten alle Beteiligten (die Redmonder und ISVs) ja demnächst ein Mini-Profile, das alle Office-Programme berücksichtigen sollten. Auf unter 500 Seiten.

Henning Behme

HENNING BEHME



[1] Frei nach Winston Churchill: „Ich implementiere nur Standards, die ich selbst entworfen habe.“



Groupware für KMU

Auch in kleinen und mittleren Unternehmen lässt sich Teamwork digital unterstützen. Aber die Anforderungen an die Groupware-Produkte unterscheiden sich deutlich von denen in Großbetrieben. Eine Marktübersicht vergleicht 16 kommerzielle und freie Pakete.

Seite 99



Egal, ob Daten versehentlich gelöscht oder bewusst versteckt wurden – File Carver sind in der Lage, auch für immer verschwunden geglaubte Informationen zu rekonstruieren. Mittlerweile existieren sogar praxistaugliche Open-Source-Werkzeuge.

Seite 56

Groovy + Java = Grails 1.0

Das in Insiderkreisen begeistert gefeierte Grails hat im Alter von drei Jahren das 0.x-Stadium hinter sich gelassen und kann sogar schon Content Negotiation. Das Werkzeug der Wahl für schlanke Webanwendungen?

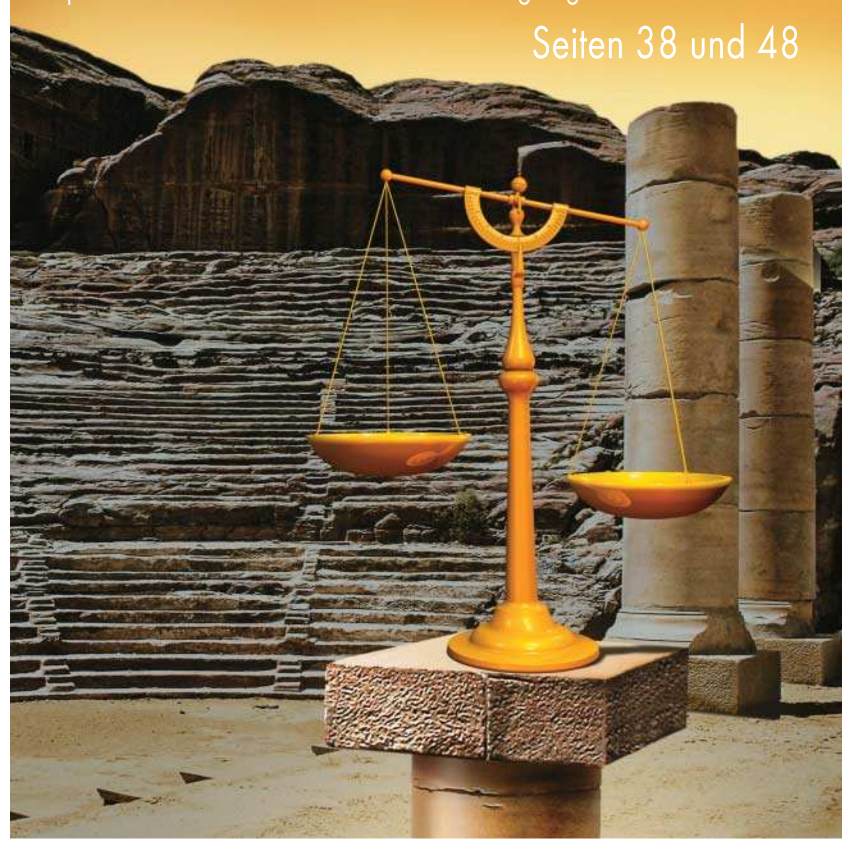
Seite 137



Software für Onlineforen

Seien es Diskussionen über Politik und Kunst, die Erörterung technischer Probleme oder einfach nur ein erweiterter Kundensupport – Onlineforen haben schon lange vor dem Web 2.0 die Benutzer zum Mitmachen animiert. Welche Software dahintersteckt und wo juristische Fallstricke für die Betreiber ausgelegt sind.

Seiten 38 und 48



Software entwickeln für Apples iPhone

Wenn Apples iPhone sein Potenzial als Business-Handy entfalten soll, sind mehr Anwendungen gefordert. Das jetzt veröffentlichte Software Developer Kit soll den nötigen Entwicklungsschub bringen. Es unterstützt native Anwendungen für iPhone und iPod Touch.

Seite 131



April, April

(Internet: Bund plant „Netz des Vertrauens“ auf IPv6-Basis; *iX* 4/08; S. 52)

Sie könnten zu meinem Wohlbefinden beitragen, indem Sie meine Vermutung bestätigen, dass das orwellianisch benannte „Netz des Vertrauens“ ein Aprilscherz ist.

SIMON THUM, VIA E-MAIL

Da den Politriksern und deren Zuträgern so einige denk- beziehungsweise merkwürdige Dinge einfallen, muss ich diesen Artikel nicht unbedingt den aprilösen Scherzen zuordnen. Oder?!?

JÖRG K. SEIFERT, OLDENBURG

Ist das der Aprilscherz oder hat das tatsächlich wahre Hintergründe?

Wäre schön, wenn sich nicht alle Schreckensszenarien bewahrheiten würden.

ANDREAS BITTNER, VIA E-MAIL

Die drei Leser liegen – wie viele andere – mit ihren Hoffnungen respektive Vermutungen richtig: Es handelt sich bei der Meldung um den diesjährigen Aprilscherz. Derzeit sind uns keine derartigen Pläne bekannt. (d. Red.)

GPS nicht per se langsam

(Forschung: WLAN und Roboter auf dem Vormarsch; *iX* 4/08; S. 20)

Ich muss bezugnehmend auf den Artikel „Gut eingebettet“ einen schwerwiegenden Fehler korrigieren: Die Einwahl in GPS ist nicht systembedingt langsam, sondern nur durch die Anforderung, ohne Benutzereingabe automatisch herauszufinden, wo man sich befindet – und zwar überall auf der Welt. Wenn man diese Informationen zur Verfügung stellt – bei früheren GPS durch die Eingabe des nächsten Ortes, heutzutage via A-GPS und dGPS, welche jeweils einen GSM-Sendemast beziehungsweise einen nahen Referenzstandort verwenden – funktioniert es praktisch ohne Verzögerung. Die weite Verbreitung automatischer Positionsbestimmung sollte GPS nicht zum Nachteil gereichen ;-) Diese Anforderung kann die WLAN-Lokalisierung klarerweise nicht bieten.

Ich hatte die Gelegenheit, das System von Fraunhofer persönlich circa eine Stunde zu testen und bin extra deswegen von Wien angereist. Mein Eindruck ist, dass es sich um ein komplementäres System zu GPS handelt: es funktioniert sehr gut in engen Straßen, wo GPS schlecht arbeitet; neigt jedoch auf großen Plätzen zum Hin- und Herpendeln – ebenso wie in Gebäuden. Die Erkennung, in welchem Raum man sich befindet, funktioniert ganz gut – innerhalb des Raums ist eine Lokalisierung aber praktisch nicht möglich.

Der große Nachteil des Fraunhofer-Systems ist aber, dass jede Stadt (Aufwand circa 8 Manntage für die Nürnberger Innenstadt) sowie jedes einzelne Gebäude vermessen werden und diese Messung regelmäßig wiederholt werden muss – zumindest einmal im Jahr, wahrscheinlich wesentlich öfter. Das

DER DIREKTE DRAHT ZU iX

Redaktion iX
Postfach 61 04 07
30604 Hannover

Fax: 05 11/53 52-361
E-Mail: <user>@ix.de
Web: www.ix.de

Direktwahl zur Redaktion: 05 11/53 52-387

Für telefonische Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion wie gewohnt während der Lesersprechstunde zur Verfügung. Und zwar:

Montag bis Freitag, 11 bis 12 Uhr

Bitte nur während der genannten Zeiten anrufen und möglichst die angegebene Durchwahl benutzen.

<Durchwahl>	<user>	
-387	post	Redaktion allgemein
-377	avr	(André von Raison)
-590	ck	(Christian Kirsch)
-387	cle	(Carmen Lehmann)
-374	hb	(Henning Behme)
-379	jd	(Jürgen Diercks)
-386	js	(Jürgen Seeger)
-367	ka	(Kersten Auel)
-153	mm	(Michael Mentzel)
-787	mr	(Michael Riepe)
-373	rh	(Ralph Hülsenbusch)
-689	sun	(Susanne Nolte)
-368	un	(Bert Ungerer)
-535	ur	(Ute Roos)
-384	wm	(Wolfgang Möhle)

Listing-Service:
Sämtliche in iX seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich:
ftp.heise.de/pub/ix/

macht es nicht kompetitiv zu GPS, da hohe Initialkosten anfallen. Nur wenn das System eine kritische Masse erreicht und die laufenden Messungen z. B. via GPS-Referenz vollständig automatisiert werden können und eine approximative Simulation der Gebäudeabschirmung aufgrund von existierenden Bauplänen geschaffen wird, wäre dieses System kompetitiv. Bis dahin ist es aber noch ein langer, steiniger Weg, und so positioniert Fraunhofer das System auch als Nischenanwendung und nicht als GPS-Ersatz – und so sollten Sie es auch beschreiben!

DR. ALEXANDER K. SEEWALD, VIA E-MAIL



2D-Code-Reader für iPhone

(World Wide Web: Der mobile Link ins Internet; *iX* 3/08; S. 116)

Habe mich gewundert, dass in Ihrem sehr interessanten Code-Tagging-Artikel mit keinem Wort die Aachener Firma Gavitec erwähnt wurde. Immerhin hat Gavitec (www.mobiledigit.de) mit dem NeoReader (www.neoreader.com) den zurzeit weltweit technisch besten Code-Reader auf dem Markt. Er liest sowohl 1D- als auch 2D-Codes und kann bis zu 7 unterschiedliche (also auch proprietäre) Codes lesen. Weiterhin beherrscht der NeoReader nicht nur direktes, sondern auch indirektes Code-Reading. Bei der direkten Methode (Kayawa, Zxing, BeeTagg usw.) ist die Adresse im Code selbst abgebildet, während beim indirekten System ein Server zwischengeschaltet ist, um Codes „in Echtzeit“ über das Internet zu validieren.

Im Besonderen ist das indirekte System aber günstig für Marketinganalysen, da auf diesem Wege Nutzungsdaten der Konsumenten mitgeliefert werden. Wer klickt was wann an, das sind die interessanten Informationen für die Markenartikler und die große Chance auch für die Mobilfunkunternehmen, finanziell am Code-Tagging-Geschäft zu partizipieren.

Übrigens will AT&T noch in diesem Monat bekanntgeben, dass der NeoReader vorinstalliert in den USA auf dem iPhone ausgeliefert wird. Diese Nachricht wird die kleine Firma aus Deutschland sicherlich schlagartig bekannt machen.

Großes Vertrauen in die Gavitec-Technik setzt derzeit auch die Welt-Airline-Vereinigung IATA. Bis zum Jahr 2010 sollen alle Flughäfen dieser Erde mit 2D-Handy-Boarding-Systemen (sogenannte Exio-Scanner, die 2D-Codes vom Handy-Bildschirm ablesen können) von Gavitec bestückt werden. Papiertickets und Boardingtickets fallen weg. Damit will die IATA jährlich 3 Milliarden Euro einsparen.

RAFAEL TORRES, KÖLN

Ergänzungen und Berichtigungen

(Vorschau: Rundum-sorglos-Pakete für KMU; *iX* 4/08; S. 170)

Der Artikel über die Linux-Konkurrenz zu Microsofts Small Business Server erscheint aus redaktionellen Gründen erst in Ausgabe 6/08.

(Wirtschaft: Zuwachs; *iX* 3/08; S. 40)

Der in der Ausgabe 3/2008, Seite 40, gemeldete Umsatz der hiesigen GmbH von SAS Institute in Höhe von 152 Mio. Euro für 2006 ist nicht mit dem Umsatz von SAS Deutschland gleichzusetzen. Bis 2006 hat SAS den Umsatz der SAS GmbH mit Sitz in Deutschland veröffentlicht (Umsatz 2006: 152 Mio. Euro), der zusätzlich Einnahmen der organisatorisch hier angesiedelten EMEA-Zentrale enthielt. Durch die Schließung der EMEA-Zentrale in Deutschland war es für 2006 zum ersten Mal möglich, Umsatzzahlen (2006: 90 Mio. Euro) ausschließlich für SAS Deutschland auszuweisen.

Die *iX*-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Einsenders wieder, nicht die der Redaktion.

Novells 23. Brainshare in Salt Lake City

Tanz mit Fossa

Detlef Borchers

Nach den Turbulenzen im Vorjahr versuchte Novell den Besuchern mit dem „Fossa Project" Langzeitstrategie zu vermitteln. Aber auch ohne diese „Vision" zeigte die Brainshare (Motto: „Making IT Work as One"), dass Novell mit den Themen Hardwarevirtualisierung und Identitätsmanagement auf einem guten Weg ist.

Teilt man die Welt in praktische Quadranten auf – wie es IT-Analysten gerne machen –, so gibt es Sektoren für Firmen, die im Wesentlichen bei „Closed Source" bleiben wie Microsoft und solchen, die auf „Open Source" (OSS) setzen wie Red Hat. Die anderen beiden Quadranten bilden die interessanten Mischungen, etwa Apple mit einem Betriebssystem, das quelloffene Wurzeln hat.

Mit der Basis Linux, eigener Managementsoftware als Überbau sowie als Querstreben einen Pakt mit Microsoft und einen mit SAP, gibt sich Novell gerüstet für die Zukunft. Anders als 2007, als das Microsoft-Abkommen im Mittelpunkt stand, gab man sich heuer viel Mühe, diese Mischung als „ganzheitliche" Strategie zu verkaufen und fand damit wohl Akzeptanz bei den rund 5000 Teilnehmern. Unter ihnen waren deutlich mehr Linux-Programmierer als früher, sodass ein Klischee auch visuell bestätigt wurde: Den klassischen Netware-Admin mit kleinem Bauch ersetzen drahtige Linux-Cracks, die in den Pausen Spaß am Gerät haben.

Viele neue Namen

Sogar einen Namen hatte man bei Novell für die neue, ganzheitliche Strategie gefunden. Auf „Fossa Project" getauft, erinnerte der Name sowohl an „Free and Open Source Software Architecture" als auch an eine kleine, agile, auf Madagaskar lebende Raubkatze. Mit Fossa definiert sich Novell als agile Firma mit einer Strategie, die bis etwa 2015 reichen soll. Orchestration, Compliance und Collaboration: Novells Beschreibung von Fossa ist voller „Buzzwords", die in den kommenden Jahren Produkte mit Leben füllen sollen. In seiner Keynote beschrieb Novells Technikchef Jeff Jaffe das Fossa-Projekt: „Linux ist die Basis unserer Virtualisierungslösung. Es wird eine p-Distro – ein Linux-Kern sowie ein abgespecktes Betriebssystem – geben, die die Hardware kontrolliert und virtuelle Maschinen startet. Auf dieser Distro laufen virtuelle Maschinen oder v-Distros, gesteuert von einem mit dynamischen Policies arbeitenden Identitätsmanagement. Das Resultat: Eine durchgehende Orchestrierung von Hard- und Software."

Wie das alles funktionieren soll, zeigte Novell am dritten Tag der Brainshare mit einem SAP-Beispiel und der Managementsoftware Zenworks Orchestrator. Anwender, die sich morgens in SAP einloggen, benötigen zusätzliche Rechenleistung. Virtuelle Maschinen werden mit der Software passend zu den Nutzerberechtigungen gestartet und wieder geschlossen, wenn der Bedarf zurückgeht. Für die Demonstration bekam Jaffe großen Beifall von den Technikern, die in der neuen Fossa-Terminologie „Compliance Officers" heißen und nicht länger die vielgescholtenen Administratoren sind. Beifall gab es auch, als am Ende der ersten Keynote-Runde die amerikanische SAP-Managerin Pat Hume verkündete, dass Novells Enterprise Linux die zentrale Systemplattform für SAPs Einsteigerlösung Business All-in-one sein soll, die SAP bis zum Jahr 2010 über 100 000-mal installieren möchte. Zwar hatte SAP ein ähnliches Abkommen mit Microsoft kurz zuvor auf der Cebit verkündet, doch sieht man sich bei Novell durch die Integration in den Zenworks Orchestrator im Vorteil, der direkt an SAPs Netweaver andockt.

Überhaupt, Microsoft: Während das Abkommen im letzten Jahr auch unter den Brainshare-Teilnehmern umstritten war, die OSS-Fraktion in einem benachbarten Hotel sogar eine Protestveranstaltung abhielt, wurden die Redmonder mit ihrem großen Stand auf der Begleitmesse ausnehmend freundlich begrüßt. Laut Novell brachte die Kooperation Kunden (zurück), die man sonst nicht erreicht hätte: die Ladenketten Wal-Mart und Office Depot sowie die HSBC-Bank entschieden sich so für Novell. Wichtigstes Produkt der Allianz ist wohl die Virtualisierungslösung für Windows Server 2008, die erwähnte Compliance Officers betreuen dürfen. Außerdem sei der Auftritt von Kim Cameron erwähnt, der bei Microsoft als Chefstratege für das Identitätsmanagement mit Novell-Managern wie Dale Olds vom Bandit-Projekt über den „Identitäts-Bus" diskutierte. Ob in Firmennetzen oder im Web, überall soll ein Anwender ID-Cards einsetzen können, bei denen er entscheidet, welche Teile seiner Identität er preisgeben will und welche vertraulich sein sollen. Aus deutscher Sicht mag hier von Interesse sein, dass Novell mit Atos Origin gemeinsam Directory- und Compliance-Lösungen vermarkten will, mit denen Firmen staatliche Auflagen einhalten können. Neue Kunden dieser Partnerschaft sind der deutsche Sender Premiere und die spanische Arbeitsagentur Institutode Empleo Servicio Publico (INEM).

Ausblick auf SLES 11

Neben der Ankündigung zahlreicher Kooperationen nannte Novell erste Pläne für sein kommendes Enterprise Linux 11 auf Basis des Linux-Kernels 2.6.27. Neben der üblichen Aufteilung in SLES (Server) und SLED (Desktop) wird es je eine Version für Thin Clients und für Appliances geben. Daneben will man einen Schul-Desktop zusammenstellen, den Lenovo und Dell zusammen mit ihren Laptops vermarkten. Für Umsteiger von alten Unix-Systemen wird SLES 11 mit Oracles OCFS ein Posix-konformes Dateisystem erhalten. Die vagen Angaben sind nach Novell reine Orientierungsmarken für die Entwickler, sich diesem oder jenen Open-Source-Projekt anzuschließen. Niemand Geringeres als der Entwicklungschef Jeff Jaffe gab sich vorsichtig, was die viel beschworene Integration von OSS-Projekten bei Novell anbelangt: „Die Arbeit der Community ist toll, aber wenn die Innovationen in viel zu viele Richtungen gehen, dann verfranzt man sich. Wir müssen die Vorgaben machen und die Fahrtroute abstecken."

Ob diese Vorgaben ankommen und bei Novell zu einem „ganzheitlichen" Ansatz führen, der die Produktion von offener wie proprietärer Software ermöglicht, steht in den Sternen: Als Raubkatzen konnten sich Fossas nur auf Madagaskar halten, wo sie keine natürlichen Feinde haben. Zur Brainshare präsentierte Novell mit Joe Brockmeier erstmals einen „Community Manager", der als Dolmetscher zwischen Management und der Entwicklern potenzielle Irritationen aus dem Wege räumen soll. Er gab sich überzeugt, dass bald alle großen Firmen solche Community-Manager einsetzen würden – und das nicht nur als „Evangelisten", die Anwender von Linux überzeugen. So stehen Novell spannende Zeiten bevor. Das meinen auch die Akademiker, die im Rahmen eines Technologie-Austauschprogrammes erstmals an der Brainshare teilnehmen konnten. Ein Neuling erklärte sein Eintauchen in das Klassentreffen der Administratoren aus aller Welt: „Man kann hier Novells Technologien studieren. Man kann aber auch Novell als Technologie studieren. Das ganze Gerede um Mixed-Source-, Semi-Source- und Closed-Source-Softwarefirmen ist doch Unsinn. Kein Softwarehersteller wird zukünftig daran vorbeikommen, OSS-Entwicklungsprojekte zu integrieren, auch Microsoft oder SAP nicht. Novell ist somit ein Studienobjekt für die Reibungsverluste, die dabei auftreten können." (avr)

VR 2008: Neue Interaktionstechniken im Einsatz

Händedruck in 3D

Christian Geiger

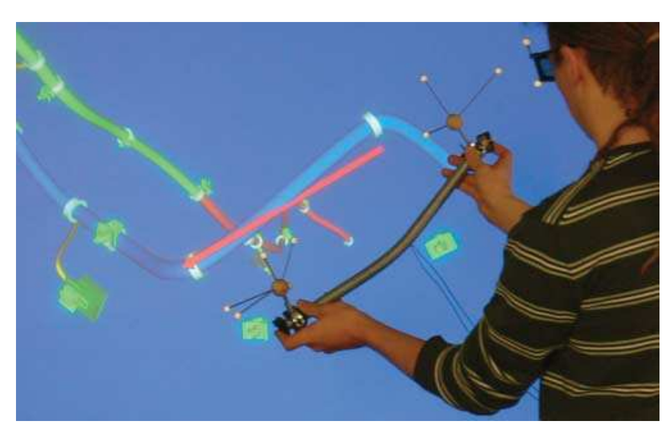
Neue Eingabegeräte und die Interaktion zwischen realen und virtuellen Menschen waren Thema vieler Vorträge auf der VR 2008 in Reno. Industrielle Anwendungen zeigen, dass die Erweiterung der Realität im Kommen ist.

Eine Woche lang traf sich die internationale VR-Gemeinde in Reno, um sich über neue Techniken in den Bereichen 3D-Schnittstellen, virtuelle Realität sowie haptische Ein- und Ausgabegeräte auszutauschen. Die starke deutsche Beteiligung belegt, dass deutsche Forscher eine führende Rolle bei der Entwicklung neuer VR-Techniken spielen.

Neue Aufgaben erfordern neue Eingabegeräte. Ein amerikanisches Team stellte ein virtuelles Boreskop mit haptischem Feedback vor. Boreskope sind kostspielige technische Endoskope, die man beispielsweise zur Inspektion von Motorelementen im Flugzeugbau verwendet. Zum Training solcher Aufgaben wurde ein Metallschlauch in einen Holzkasten geführt und dort mit einer optischen Maus verbunden, um die Position des Schlauches zu erfassen. Das haptische Feedback erfolgte über Servomotoren, die eine Curryklemme aus dem Segelsport steuern und so die Bewegung des Schlauches computergesteuert einschränken. Erste Tests ergaben bessere Ergebnisse mit haptischem Feedback.

Als Ergebnis einer studentischen Abschlussarbeit stellte die Fachhochschule Düsseldorf ein Eingabegerät vor, das zwei Griffe mit Tastern durch eine 50 cm lange Biegefeder verbindet. Die beiden Enden sind mit Infrarot reflektierenden Kugeln versehen, sodass ein Tracking-System sie verfolgen kann. Das System dient zur Eingabe bei der Simulation von Kabelschläuchen. Auch wenn sich die flexible Verbindung nicht exakt wie ein Schlauchelement verhält, kann man mit dem Gerät recht intuitiv spezielle Aufgaben bei der Schlauchsimulation erledigen (s. Abbildung).

Head-Mounted Displays werden oft wegen ihrer geringen Auflösung und des kleinen Sichtwinkels kritisiert. Ein neues Device von Sensics (www.sensics.com) bietet eine Full-HD-Auflösung und einen Sichtwinkel von bis zu 180 Grad horizontal beziehungsweise 80 Grad vertikal. Durch ein Feld gekachelter Mikro-Displays mit Linsenprismen kann man unterschiedliche Auflösungen und Sichtfelder konfigurieren, indem man mehr oder weniger Felder kombiniert. Durch die OLED-Technik sind die Geräte sehr leicht (ca. 50 g pro Auge), besitzen eine hohe Grundhelligkeit und einen guten Kontrast. Ein einzelnes Modul kostet circa 15 000 US-$, und als Preis für ein komplettes HMD nannten die Aussteller eine Größenordnung ab 25 000 $.



Mit beiden Händen bedient der Anwender dieses Eingabegerät für Schlauchsimulationen.

Virtuelle Menschen in der Industrie

Beiträge zu industriellen Anwendungen in der VR zeigen, dass die Technik den Weg aus den Laboren der Universitäten heraus gefunden hat. Forschern der Bauhaus-Universität Weimar ist es in Zusammenarbeit mit VW gelungen, ein System zum Testen neuer Interaktionstechniken in zukünftigen Fahrzeugzellen zu entwickeln. Da die Simulation künftiger Bedienkonzepte auch die Interaktion mit dem Beifahrer erfordert, verfolgt das System die Kopf- und Handbewegungen zweier Personen gleichzeitig und stellt passende Avatar-Modelle zur Verfügung, sodass beide Benutzer die Handlungen des anderen in der virtuellen Welt beobachten können.

Forscher der Universität Graz präsentierten eine industrielle Anwendung, die virtuelle Objekte direkt in reale Szenen einbettet. Diese Technik heißt „Augmented Reality“ (AR) und gilt als vielversprechende Erweiterung der VR. Das in Graz entwickelte System zur Abnahme für Industriebauten ermöglicht eine schnelle Überprüfung, die vor Ort mit einem fahrbaren Teleskopgestell erfolgt, auf das ein Touchscreen mit Videokamera montiert wurde. Mit dem System ließen sich Abweichungen zu den ursprünglichen Plänen direkt ins Videobild einblenden und konnten so schneller festgestellt werden als durch den Einsatz eines Mini-Laptops (UMPC) oder mittels Head-Mounted Display.

Ein Schwerpunkt war die Modellierung virtueller Menschen. Der Einsatz solcher Modelle im Rahmen von Ergonomieuntersuchungen in der Automobilindustrie ist ein wichtiger Anwendungsbereich von VR. Benjamin Lok von der Universität Florida hat sich auf Untersuchungen mit 3D-Avataren spezialisiert und präsentierte Ergebnisse seiner Forschung. Für die Kommunikation zwischen Mensch und 3D-Avatar wurde ein Werkzeug vorgestellt, das einen Review der erfolgten Interaktion in medizinischen Gesprächssituationen ermöglicht. Studenten konnten so ihre Kommunikation mit virtuellen Patienten überprüfen und verbessern. Die bei Untersuchungen notwendige „berührbare“ Interaktion ermöglichen Loks „Mixed Reality Humans“, bei denen lebensgroße Puppen als Untersuchungsobjekt dienen und über ein HMD virtuell Reaktionen des simulierten Patienten dargestellt werden.

Ein Kernproblem in VR- und AR-Welten ist das Tracking des Benutzers und einzelner Objekte. Als naheliegende Lösung verwenden Entwickler spezielle optische Marker oder nutzen teure Sensoren. Seit Langem arbeitet man daher an alternativen Techniken zur markerlosen Bilderkennung in Echtzeit. Forscher der Universität Darmstadt haben in einem hybriden Ansatz Inertialsensoren mit einem kantenbasierten Bilderkennungsverfahren kombiniert. Dabei messen Sensoren die Bewegung und Orientierung einer Videokamera. Diese Daten werden mit dem aktuellen Kamerabild abgeglichen und ermöglichen eine effiziente Erkennung von Merkmalen wie Ecken und Kanten. Der Vergleich mit einem vorab gespeicherten 3D-Modell erlaubt die robuste und schnelle Erkennung einer Szene.

Obwohl sich VR und AR-Techniken in Teilgebieten bereits durchgesetzt haben, werden kommerzielle Produkte auf breiter Anwenderebene trotz vieler spannender Ergebnisse noch auf sich warten lassen. Die nächste Konferenz soll im März 2009 in Lafayette, Louisiana, stattfinden. (ka)



JSFDays 08: Mehr Schnittstellen für RIAs

Neue Gesichtsfelder

Oliver Becker

Das Web-Framework Java Server Faces erfreut sich wachsender Beliebtheit und hat seit Kurzem seine eigene Konferenz.

Mehr als 160 JSF-Interessierte folgten der Einladung Inrias, Initiator des Projekts Apache Myfaces, Mitte März nach Wien. So viele, dass der Veranstalter kurzfristig größere Räumlichkeiten organisieren musste.

Zu Beginn der Konferenz benannte Ed Burns, Lead der JSR Expert Group für Java Server Faces (JSF) 2.0, in seiner Keynote den Fokus für das Web-Framework: die Bereitstellung mächtiger Nutzerschnittstellen für Rich Internet Applications (RIA). Mithilfe solcher Schnittstellen sollen sich Webanwendungen entwickeln lassen, die Desktop-Programmen ebenbürtig sind.

Vor- und Nachteile der Browser-Plug-ins

Dementsprechend drehte sich ein Großteil der Beiträge um RIAs. Mehrere Vortragende stellten die Ajax-fähigen Komponentenbibliotheken Rich Faces, ADF Faces und ICE Faces vor. Max Katz verglich JSF mit den alternativen Techniken Flex und JavaFX, die spezielle Browser-Plug-ins benötigen, in der die Ausführung der Anwendungen erfolgt. Das hat den Vorteil, dass eine solche Applikation unabhängig vom Browser immer gleich aussieht. Allerdings sind separate Plug-ins nicht immer erwünscht, und auch Suchmaschinen können nicht auf sie zugreifen.

Stefan Schuster demonstrierte schließlich am Beispiel von mind24.com die Mächtigkeit reiner Javascript-Anwendungen. Dass Scripting mehr bedeutet als Browser-Javascript, zeigte Kito Mann, der Möglichkeiten zur Entwicklung serverseitiger Komponenten auf der Basis von Skriptsprachen vorstellte.

Mehr Frameworks für mehr Komfort

Drei weitere Vorträge beschäftigten sich mit den JSF-Integrations-Frameworks Myfaces Orchestra, JBoss Seam und Apache Shale. Vor allem Seam und Orchestra wurden ausführlich und praxisnah präsentiert und fanden entsprechenden Anklang beim Publikum. Beide fügen unter anderem den JSF-Standard-Scopes einen Conversation-Scope hinzu und ermöglichen die Validierung von Eingabedaten auf der Basis von JPA-Annotationen. Insbesondere Seam bietet darüber hinaus eine Vielzahl weiterer Funktionen, die innerhalb des Vortrags nur kurz angerissen werden konnten und einen genaueren Blick wert sind.

Der kurzweilige Beitrag zu Shale zeigte die Kehrseite mancher Projekte. Obwohl viele Anwender dieses Framework erfolgreich einsetzen, ist dessen Zukunft mangels aktiver Entwickler ungewiss. Immerhin haben die mit Shale gesammelten Erfahrungen und Ideen andere Projekte inspiriert und werden auf diese Weise fortbestehen.

Jürgen Höller sprach über die sehr gute JSF-Integration in Spring. Weitere Vorträge stellten Werkzeuge für das Testen von Webanwendungen sowie die Steuerung der Ressourcenkonfiguration mithilfe von Weblets vor. Manfred Geiler präsentierte eine clevere Idee, mit der sich Domänen-Objekte aspektorientiert, jedoch ganz ohne echte AOP-Sprachmittel um UI-spezifische Eigenschaften und Aktionen erweitern lassen.

JSF 2.0 steht in den Startlöchern

Mit großem Interesse erwarteten die Konferenzteilnehmer die Session zu den Eigenschaften der kommenden Version JSF 2.0. Ed Burns listete die aus dem JSR 314 bereits bekannten Top-5-Anforderungen und erste Lösungsansätze auf: vereinfachte Komponenten-Implementierung, Ajax-Unterstützung, eine standardisierte Seitenbeschreibungssprache (Facelets), die reduzierte Konfiguration sowie eine verbesserte Kompatibilität zwischen unterschiedlichen Komponentenbibliotheken. Zu den weiteren Zielen zählen ein verbessertes State-Management, REST-Fähigkeit, minimaler Deployment-Aufwand und zusätzliche Scopes. Ein erster öffentlicher Entwurf für JSF 2.0 soll spätestens zur JavaOne Ende April erscheinen. Lebhafter wurden dann der Entwicklungsprozess selbst und die Einbindung der Öffentlichkeit diskutiert. Vorschläge vonseiten der Konferenzteilnehmer, das Archiv der internen Mailingliste zu öffnen oder wöchentliche Zusammenfassungen über die Arbeit der Expert Group zu veröffentlichen, wurden positiv aufgenommen.

Nach der diesjährigen erfolgreichen Premiere kann man mit Sicherheit davon ausgehen, dass es eine Folgekonferenz JSFDays 09 geben wird. Alle Vorträge sind über die Konferenz-Homepage (conference.irian.at) abrufbar. (ka)

Datenklau im RAM mit iPod & Co.

Zweckentfremdet

Stefan Middendorf

Wie man mit einem umfunktionierten iPod ein Notebook bootet und dessen Hauptspeicher ausliest, war nur eines der thematischen Highlights der diesjährigen CanSecWest.

Die bereits zum neunten Mal veranstaltete CanSecWest zählt mit der Black Hat/Defcon zu den größten IT-Sicherheitskonferenzen Nordamerikas. Rund 400 Teilnehmer fanden sich diesmal in Vancouver ein.

Rich Cannings von Google berichtete über Techniken, Flash-Komponenten für Cross-site-Scripting-Angriffe zu missbrauchen (Cross-site Flashing). Diese Technik beruht darauf, dass die Flash-eigene Programmiersprache Actionscript das Ausführen von Javascript-Code im Browser ermöglicht. Übergibt man der URL zum Abruf der Flash-Datei Parameter mit Javascript-Fragmenten, kann bei Vorhandensein einer entsprechenden Schwachstelle im Actionscript-Code der Javascript-Code im Browser des Opfers zur Ausführung kommen. Adobe hat zwar Ende letzten Jahres einen Fix für das Flash-Plug-in herausgebracht, der die Ausnutzung erschwert, das große Problem ist jedoch, dass viele Flash-Authoring-Tools verbreitet sind, die immer noch verwundbare Actionscript-Fragmente in die erzeugten Flash-Komponenten einbauen.

Ein weiterer Vortrag beschäftigte sich mit Cold-Boot-Attacken. Hierbei nutzt man dem Umstand aus, dass RAM-Chips nach dem Abschalten des Stroms noch für eine Weile ihren Zustand erhalten. Schaltet man das System innerhalb dieser Zeitspanne wieder ein und sorgt dafür, dass die alten Speicherinhalte beim Hochfahren nicht überschrieben werden, lassen sich diese auslesen. Das ermöglicht das Abgreifen sensibler Informationen wie Passwörter, die sich vor dem Ausschalten im RAM befanden. Die „Überlebensdauer“ der Daten hängt vom Typ der RAM-Chips und vom Computer ab. In einigen Fällen waren die Daten sogar noch nach fünf bis zehn Minuten lesbar.

iPod zum Hacken

Bill Paul führte vor, wie er ein Notebook nach dem Ausschalten von einem umfunktionierten iPod neu bootete, auf dem sich ein von ihm entwickeltes Minibetriebsystem befand. Dieses lässt den Hauptspeicher weitgehend unberührt und gestattete das Kopieren des Notebook-RAMs auf den iPod.

In einem Lightning Talk nannte der *nmap*-Entwickler Fyodor die neuen Features seines Netzwerk-Scanners. So ist die Paketrate jetzt fest einstellbar und die Betriebssystemerkennung wurde komplett neu entwickelt.

Den Abschluss der Veranstaltung bildete ein Thema ganz anderer Art. Der Psychologe Eric Shaw und sein Kollege Scott Larson stellten ihren Ansatz vor, aus der Analyse anonymer Droh-E-Mails ein psychologisches Profil der Absender abzuleiten. Hierzu werden unter anderem die Häufigkeit bestimmter Wortgruppen (z. B. Negierungen, Bewertungen, rhetorische Fragen) sowie die Satz- und Absatzstruktur herangezogen, um auf psychische Eigenschaften und die Stimmungslage des Absenders zurückzuschließen. Diese Methode kann etwa dazu dienen, Innentäter zu identifizieren, die das eigene Unternehmen erpressen. So berichteten die Referenten über Fälle, in denen Mitarbeiter von Unternehmen anhand solcher Profile die Absender spontan identifizieren konnten. (ur)

Mit wenig Geld Telefongespräche abhören

Von Lauschern und Routern

Tobias Klein

Wer etwas über Router-Forensik, GSM-Hacking oder Webapplikations-Sicherheit erfahren wollte, war auf der diesjährigen Black-Hat-Konferenz in Amsterdam bestens aufgehoben.

In seinem Vortrag „Client-side Security“ bot Petko D. Petkov eine Übersicht über diverse Schwachstellen und Probleme innerhalb weit verbreiteter Client- und Webanwendungen wie Skype, Googles Gmail, BT Home-Routern sowie Second Life. Neben der Skizzierung der Schwachstellen gab er ebenfalls zu bedenken, dass Browser-Rootkits wohl nicht mehr allzu lange auf sich warten lassen. Heutige Browser verfügen über diverse Schnittstellen und Erweiterungsmöglichkeiten, die sich geradezu für die Entwicklung solcher Schadsoftware anbieten.

Dass viele Hersteller von Anti-Viren-Produkten sich nicht gerade durch sichere Software hervortun, ist mittlerweile bekannt. So vergeht kaum ein Monat ohne neu veröffentlichte Schwachstelle in einem Anti-Viren-Produkt. Feng Xue, in einschlägigen Kreisen besser bekannt unter dem Pseudonym Sowhat, vermittelte den Zuhörern einen Einblick in die Angriffspunkte und Möglichkeiten zur Entdeckung und Ausnutzung solcher Schwachstellen.

Chema Alonso und Jose Parada Gimeno gingen in ihrem Vortrag auf ein Thema der Webapplikations-Sicherheit ein, das in der Regel recht stiefmütterlich behandelt wird: LDAP Injection. Anhand verschiedener Beispiele mit OpenLDAP und Microsofts ADAM demonstrierten sie eindrucksvoll, welche Möglichkeiten diese Angriffstechnik bietet und dass es sich dabei keineswegs um eine theoretische Schwachstelle handelt. Prüfen Webapplikationen die Eingaben nicht, so lassen sich ähnlich wie bei SQL Injection vertrauliche Informationen auslesen oder Authentifizierungsmechanismen umgehen.

Eines der Highlights der Konferenz war Felix Lindners Vortrag über die Möglichkeiten der forensischen Analyse von Cisco-Routern. Lindner stellte ein neues Framework namens Cisco Information Retrieval (CIR) vor, das in der Lage ist, Core Dumps von Cisco Routern einer eingehenden Analyse zu unterziehen. Das Framework kann die IOS-Prozessliste, den Hauptspeicher sowie die Heap-Strukturen aus einem Core Dump rekonstruieren. Die extrahierten Informationen werden anschließend verschiedenen automatischen Analysen unterzogen.

Framework für Fehlersuche

Dass man mit dem ursprünglich von Sun entwickelten Dtrace über mächtige Funktionen zum Troubleshooting verfügt, ist weitgehend bekannt. Nachdem die Funktion ebenfalls in Apples aktueller OS-X-Version Einzug gefunden hat, nahmen Tiller Beauchamp und David Weston dies zum Anlass, aufbauend auf Dtrace ein Framework namens RE:Trace zu erstellen, das die gezielte Suche nach Schwachstellen sowie deren Ausnutzung unter Apples Betriebssystem in vielen Bereichen unterstützen soll.

So prüft die Software, ob das IOS-Image modifiziert wurde, ob TCL-Hintertüren vorhanden sind oder ob es Anzeichen für eine Kompromittierung des Heap gibt. Zudem ist das Framework in der Lage, die sich im Speicher des Routers befindlichen Netzwerkpakete für eine weitere forensische Analyse zu extrahieren (cir.recurity-labs.com).

Ein weiteres Highlight der Konferenz war der Vortrag „Intercepting GSM Traffic“ von David Hulton und „Steve“. Nach einer kurzen Erläuterung der sich hinter dem GSM-Netzwerk verbergenden Technologien stellten die beiden eine relativ kostengünstige Lösung vor (circa 900 $), die den verschlüsselten GSM-Netzwerkverkehr passiv mitschneiden kann. Damit nicht genug, erläuterten sie anschließend, wie sich die im GSM-Netz eingesetzte Verschlüsselung A5/1 knacken lässt. Anhand vorberechneter Rainbow Tables und eines rund 2000 $ teuren Equipments sind die beiden in der Lage, innerhalb von 30 Minuten ein beliebiges Telefongespräch zu entschlüsseln. Investiere man mehr Geld in die Hardware, so die Referenten, könne der Prozess um ein Vielfaches beschleunigt werden (wiki.thc.org/gsm). (ur)

iX-Kreuzworträtsel: Die Gewinner

Dass das Lösungswort für das IT-Kreuzworträtsel aus Heft 3/08 „Bundestrojaner“ war, haben doch tatsächlich 99 % der Teilnehmer herausgefunden. Wir versprechen: Im nächsten Jahr wird’s etwas schwieriger.

Gratulieren aber möchten wir auf diesem Wege den drei ausgelosten Gewinnern eines iPod touch:
Benedikt Burgstaller-Mühlbacher, Rossbach (A)
Michael Wurzel, Bonn
Nils Janßen, Burgdorf

Software bewertet Umweltbelastung

In den meisten Unternehmen hat sich der Drucker- und Kopiergerätepark heterogen über Jahre entwickelt, als von Energieeffizienz und grüner IT noch nicht die Rede war.

Mit dem „Sustainability Calculator“ will Xerox Unternehmen dabei unterstützen, ihre Dokumente energie- und ressourcensparend zu verarbeiten. Zunächst beziffert die Software die Umweltbelastung durch vorhandene Drucker, Kopierer und Multifunktionsgeräte.

Kriterien sind dabei der Verbrauch von Energie, Papier, Wasser und Luft sowie die erzeugten Treibhausgase. Danach empfiehlt der Nachhaltigkeitsrechner nach Angaben von Xerox energie- und ressourcensparende Maßnahmen, zum Beispiel den Duplex-Druck oder den Austausch veralteter Geräte durch Multifunktionssysteme.

Im Einsatz ist der Rechner nach Angaben von Xerox bei der Northrop Grumman Corporation, einem US-amerikanischen Unternehmen, das unter anderem Systeme für die Schiff-, Luft- und Raumfahrt produziert. In einer Abteilung reduzierte man die über 2000 Drucker, Kopierer und Multifunktionssysteme auf 1100 Geräte, die nun etwa ein Viertel weniger Energie verbrauchen sollen.

Eine Vollversion des „Sustainability Calculator“ will Xerox demnächst online zur Verfügung stellen; wann genau, war nicht zu erfahren. Auch die Kosten bleiben noch im Dunkeln. Eine abgespeckte kostenlose Version, bei der man die vorhandenen und geplanten Werte für seine Gerätschaften eingeben muss, findet sich unter www.consulting.xerox.com/flash/thoughtleaders/suscalc/xeroxCalc.html. *Barbara Lange*

iX-Umfrage: Notebook wird PC-Ersatz

Eine knappe Mehrheit sieht beim beruflichen Einsatz den Laptop als vollwertigen Ersatz für einen stationären PC; 31 % der Befragten bejahten dies sogar ohne jede Einschränkung, während bei 19 % eine Docking-Station und bei 6 % ein genügend großer Bildschirm (17") als Voraussetzung genannt wurde.

Die genauen Ergebnisse der Umfrage, die parallel zur Einzelhandelspräsenz von *iX* 4/08, lief, ist der Grafik zu entnehmen. Mit Erscheinen dieses Heftes ist auf www.ix.de eine Umfrage zum Thema Voice over IP zu finden.

Nutzen Sie beruflich Notebooks als Ersatz für stationäre PCs?

Antwort	Anteil
Ja, einen stationären PC brauche ich nicht mehr.	31 %
Ja, aber nur in Verbindung mit einer Docking-Station.	19 %
Ja, aber nur mit mindestens 17 Zoll großer Bildschirmdiagonale.	6 %
Ich nutze Notebooks nur unterwegs.	28 %
Ich nutze überhaupt kein Notebook.	16 %

Gesamtstimmen: 980 (gerundet)

IBM-Förderprogramm für Studenten

Im Rahmen seines internationalen Förderungsprogramms „Extreme Blue“ will IBM Studenten in seinen Entwicklungszentren eigenständige Projekte durchführen lassen. In einem zehnwöchigen Praktikum unter Anleitung internationaler Experten des Hauses bilden je vier Studenten ein Team, das an Themen wie hybride Systeme, Verbindung zwischen realer und virtueller Welt, Workload-Management und Green Computing arbeitet.

Die auf sechs europäische Forschungs- und Entwicklungszentren verteilten Teams treffen sich am Ende des Praktikums zur Präsentation der Ergebnisse ihrer Arbeit im Herbst 2008 bei der Extreme Blue Expo in Böblingen. Letztes Jahr fand die Veranstaltung in Hursley, UK, statt. Mit dem Förderprogramm will Big Blue Studierende aus den Fachbereichen Informatik, Wirtschaftsinformatik, Elektrotechnik, Physik und angrenzenden Gebiete ansprechen, um technische Nachwuchskräfte zu gewinnen. Interessierte können sich bis zum 30. April 2008 anmelden. Das Praktikum selbst beginnt am 21. Juli 2008 und dauert bis zum September.
Nikolai Zotow

iX-Veranstaltungen

www.ix-konferenz.de.

Wer noch in den Genuss des Frühbucherrabatts für die **Forensik-Seminare** kommen möchte, sollte sich beeilen: Nur noch bis Ende April kann man 10 Prozent der Konferenzgebühren sparen. Die Veranstaltungen finden im Juni in Berlin und München statt (siehe www.ix-konferenz.de): Referent ist der bekannte deutsche Forensik-Experte Alexander Geschonneck.

Neu hinzugekommen ist die Veranstaltungsreihe **Software entwickeln mit .Net**, die im Mai und November in Essen stattfindet. Es geht um den gekonnten Einsatz von .Net 3.5, C# 3.0 und Visual Studio 2008 respektive der Vorgängerversionen. Referent ist Holger Schwichtenberg, langjähriger *iX*-Autor und auch verantwortlich für die **PowerShell-Seminare**.



Insidern bekannt als Betreiber der Site computer-forensik.org: Alexander Geschonneck, Referent der *iX*-Forensik-Workshops



Partnerschaft: Die Software für die Leistungsverrechnung virtueller Systeme von Xentro hielt Einzug in das Infrastructure Center (IC) for VMware ESX der MysoftIT. Sie verrechnet unterschiedliche Kostenarten pro Host oder Gastsystem, verteilt Gemeinkosten auf Kostenstellen oder erstellt Simulationen für definierte Abrechnungsperioden. Beide Firmen, die auch Technology Alliance Partner von VMware sind, schlossen eine wechselseitige OEM-Partnerschaft.

Aufgekauft: Mit der Übernahme der Infra Corporation baut EMC das Portfolio im Bereich des IT-Servicemanagements (ITSM) aus. EMC will die akquirierte Firma in seine Ressource Management Software Group (RMSG) eingliedern. Infra bietet mit Infraenterprise eine ITIL-verifizierte Webanwendung an, mit der Unternehmen Servicemanagement-Prozesse unternehmensweit automatisieren können.

Gemessen: NTT Europe Online, ein Anbieter von Hosting-Services, und Keynote Systems wollen in Europa zusammenarbeiten. NTT Europe Online stellt den eigenen Kunden den Service zur Web-Performance-Analyse von Keynote zur Verfügung. Das Unternehmen unterhält rund 2400 Messcomputer und mobile Endgeräte in über 240 Standorten und mehr als 160 Stadtgebieten weltweit.

x10sure: Wenn der andere einspringt

Bereits vor Jahresfrist hatte Fujitsu Siemens Computers (FSC) mit x10sure ein einfaches Hochverfügbarkeitskonzept für kleine und mittelgroße Unternehmen vorgestellt. Nun hat die zunächst für Windows auf Primergy-Blade- oder Standardserver positionierte Lösung in der Version 2.0 die VMware-Unterstützung bekommen.

X10sure, im Grunde eine abgestrippte Variante des auf RZ-Infrastrukturen ausgerichteten ASCC (Adaptive Services Control Center), dient der Überwachung kleinerer Server-Verbände und stößt bei Ausfall eines Servers automatisch den Neustart eines Ersatzservers (Spare-Server) an, der sein Boot-Image über ein iSCSI- oder FC-SAN bezieht. Der Ausfallschutz in einem solchen n+1-Konzept lässt sich zwangsläufig kostengünstiger realisieren als eine Failover-Lösung oder ein hochverfügbares Cluster mit einer doppelt angelegten Serverzahl. Diesen Preisvorteil „erkauft“ man sich allerdings mit einer im Vergleich zum Cluster etwas längeren mehrminütigen Anlaufdauer. Für die meisten Anwendungsfälle ist dieser Grad an Ausfallschutz ausreichend.

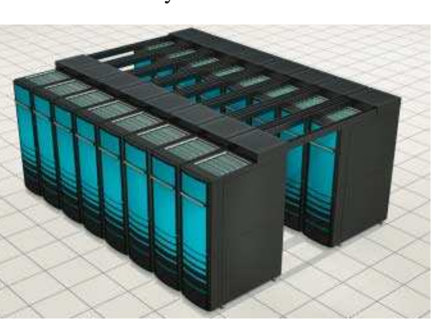
Zum Erstellen bootfähiger Server-Images kann man etwa auf die Serverview-Managementsuite der Primergy-Server zurückgreifen. x10sure überwacht die Serverfarm per ICMP, Agenten benötigt es nicht. Stellt es den Ausfall eines Produktiv-Servers fest, weist es die LUN des ausgefallenen Servers dem Ersatz-Server zu, der damit bootet und dessen Identität übernimmt. Hierzu müssen aber alle beteiligten Server (Compute Nodes) über identische Hardware und Konfigurationen verfügen. Die als RPM-Paket verfügbare Steuerungs- und Überwachungssoftware x10sure basiert auf Suse Linux (SLES 9) und ist jenseits der Produktiv- und Ersatzserver auf einem Kontrollserver beheimatet. Voraussetzung: Die Server müssen sich im selben Netz befinden. Der jeweilige Status lässt sich über ein Java-basiertes GUI verfolgen.

Eine offizielle Linux-Unterstützung – bislang nur auf Projektbasis existent – ist in Vorbereitung, ebenso die Erweiterung des N+1-Konzepts auf N+M. FSC vermarktet x10sure ausschließlich über Partner. Der Preis der kleinsten Version für fünf Server liegt bei knapp 10 000 Euro. *Achim Born*

Cray kratzt an der Petaflop-Grenze

An der Universität von Tennessee (www.tennessee.edu) wird Cray – nach eigenem Verständnis und nicht ganz zu Unrecht „die“ Supercomputer-Firma – einen neuen Superrechner installieren, dessen Spitzenleistung nah an der Petaflop-Grenze liegen soll. Damit wäre dem Unternehmen nach langer Zeit wieder ein Spitzenplatz in der Top500-Liste (www.top500.org) sicher.

Als ersten Schritt wird Cray noch in diesem Jahr einen XT4-Supercomputer installieren (www.cray.com/products/xt4/index.html). 2009 soll die zweite Ausbauphase stattfinden, die die Rechenleistung auf nahezu 1 Teraflop/s katapultiert.



Der massiv-parallele Superrechner (MPP) besteht aus einzelnen Rechenknoten (Processing Elements, kurz PE) mit je einem AMD-Opteron-Prozessor sowie 1 bis 8 GByte RAM. In Tennessee setzt Cray zunächst die neuen Quad-Core-CPUs Barcelona ein.

Als Einsatzgebiete planen die Betreiber unter anderem die Wetter- und Klimaforschung – Tornado-Vorhersage und die Untersuchung langfristiger Klimaveränderungen stehen auf dem Programm. Außerdem soll der Supercomputer die Entstehung von Supernovae und die Entwicklung von Galaxien modellieren.

Suns Niagara-2-Server mit 2 und 4 Sockeln

Ein gutes halbes Jahr nach der Einführung der Server mit Ultrasparc-T2-Prozessoren (Niagara 2) bringt Sun die ersten Systeme mit der Multiprozessorversion der 8-Kern-CPU (Codename Viktoria Falls) auf den Markt. Die offiziell Ultrasparc T2 Plus getauften Prozessoren beherrschen anders als die Ein-Sockel-Variante ein Cache-Kohärenz-Protokoll und können daher zu zweit oder zu viert in einem System werkeln. Alles andere bleibt beim Alten: Die CPUs besitzen acht Kerne mit Hardware-Unterstützung für 64 Threads, acht FPUs (Floating Point Units), acht Krypto-Koprozessoren, vier zweikanalige FB-DIMM-Controller, zweimal 10 Gigabit Ethernet und einem PCI-Express-Controller mit acht Lanes.

Eröffnen werden den Reigen der neuen T2-Enterprise-Systeme die Modelle T5140 mit einer Höheneinheit und die T5240 mit zweien. Während sich die T5140 nur durch die zwei CPUs von der Single-Sockel-Variante T5120 unterscheidet, hat die T5240 außer einem zweitem Prozessor Einschübe für nunmehr 16 2,5"-SAS-Platten mit je 146 GByte und ein Erweiterungsboard für insgesamt 128 Gbyte RAM bekommen. Mit dieser Ausstattung unterstützt das System 128 LDOMs (Logical Domains) mit je eigenen Betriebssystem-Instanzen. Der Hypervisor ist ebenso integriert wie die Hardware-Verschlüsselung und das ILOM (Integrated Lights Out Management).

Auch wenn Sun die Server am liebsten unter Solaris laufen sieht, unterstützen auch Ubuntu 7.04 Sparc und FreeBSD Sparc/64 die Niagara-Systeme. Blade-Server sollen in naher Zukunft folgen, für den Sommer sind die ersten Vier-Sockel-Systeme zu erwarten.

Aus System p und i wird Power Systems



IBM will seine beiden Server-Linien System i und System p zu den neuen Power Systems zusammenführen. Die nunmehr vollständig vereinheitlichte Familie von AIX-, Linux- und i5/OS-Servern bildet anlässlich der Einführung der neuen Power6-Prozessoren den Abschluss einer Entwicklung, die mit dem Wechsel auf die RISC-Prozessorfamilie bei der AS/400 im Jahr 1995 ihren Anfang nahm. Auch das Betriebssystem i5/OS (früher OS/400), das auf allen neuen Power-Modellen läuft, will Big Blue ein weiteres Mal umbenennen; es heißt nun „IBM i Betriebssystem“ oder schlicht und ergreifend „i“.

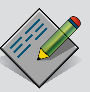
Nachdem bereits das p-Modell 570 und die Power6-Blade JS22 unter i5/OS R6V1 lauffähig waren, sollen nun die Systeme p550 und p520 sowie die kleinere Blade JS21 als erste Vertreter der vereinten Power-Systems-Familie unter AIX, Linux und i laufen.

Zudem führt IBM zwei neue Systeme ein. Den Power 595 mit 32 Dual-Core-Power6-CPUs vermarktet IBM als Unix-Server – vorerst unter AIX; Linux und i sollen im vierten Quartal 2008 folgen. Als wassergekühlten Supercomputer mit AIX oder Linux stellt IBM außerdem den Power 575 vor. Die Hydro-Cluster genannte Wasserkühlung führt die Kühlflüssigkeit durch auf den Prozessoren angebrachte Kupferplatten zu einem ins Rack integrierten Wasser-Wärmetauscher. Die Dual-Core-CPUs konnte Big Blue dadurch auf 5 GHz hochtakten. Zudem lassen sich dadurch 224 CPUs und 3,5 TByte Arbeitsspeicher – verteilt auf 14 Knoten – in einem Rack unterbringen. Jeder Knoten soll mit seinen 16 CPUs und 256 GByte RAM 600 GFLOPS erreichen. Beide Systeme sollen am 6. Mai verfügbar sein.

Von der Umstrukturierung der Server-Familien verspricht sich IBM vor allem eine vereinfachte Preisgestaltung – für System-i-Kunden seien die Hardware- und Wartungskosten damit auf dem deutlich niedrigeren Niveau der Unix- respektive Linux-Systeme angekommen. Zudem erhöht sich die Zahl der darauf unter i, AIX oder Linux lauffähigen Applikationen auf über 15 000.

Berthold Wesseler/sun

KURZ NOTIERT



Geschluckt: Nimsoft hat Indicative Software gekauft. Mit diesem Schritt erweitert der Anbieter von Service-Level-Managementlösungen sein Portfolio um Komponenten für Business Service Management (BSM) und um Funktionen für die Überwachung von Antwortzeiten. Die Indicative-Tools bieten unter anderem Funktionen zur Service-Modellierung, zum Echtzeit-Monitoring benutzerseitiger Antwortzeiten sowie zur Analyse von J2EE- und .Net-Anwendungen.

Aufkauf: Red Hat baut die Beratungssparte mit der Übernahme von Amentra aus. Das Unternehmen verfügt unter anderem über Know-how für die Jboss-Middleware. Amentra soll künftig als unabhängige Red-Hat-Tochter seine Geschäfte betreiben.

Büroarbeiter: Mit etwas Verspätung steht jetzt mit Openoffice 2.4 eine überarbeitete Version des Office-Paketes für Linux, Solaris und Windows zum Download bereit. Neben vielen Detailverbesserungen sind neu unter anderem die Option, Dokumente im PDF/A-Standard für die Langzeitarchivierung zu speichern, relative Pfade für Links in PDF-Dateien, Verschlüsselung von Kennwörtern durch ein Master-Passwort oder – derzeit nur für die Linux-Version – 3D-Animationen bei Folienwechseln im Präsentationsmodul Calc.

Megatrend: Virtualisierung wird nach Ansicht der US-Beratung Gartner bis 2012 den größten Einfluss auf die Entwicklung der IT haben. Den Beratern zufolge hat die Virtualisierung bereits jetzt Spuren im Servermarkt hinterlassen. Beispielsweise soll sie den Absatz von x86-Servern um 4 % gedrückt haben. 2009 sollen laut Gartner-Prognose mehr als 4 Mio. virtuelle Server auf x86-Maschinen laufen. Die Zahl virtualisierter PCs soll von weniger als 5 Mio. im vergangenen Jahr bis 2011 auf rund 660 Mio. hochschnellen.

Verbessert: Lufthansa Systems konnte im Geschäftsjahr 2007 die Einnahmen um 4,1 % auf 679 Mio. € steigern. Dabei betrug der Umsatzanteil mit Kunden außerhalb der Muttergesellschaft 41 %. Das operative Ergebniss hat sich mit 23 Mio. € allerdings halbiert.

Großer Knoten: DE-CIX, der Internet-Austauschknoten in Frankfurt/M. (www.de-cix.net), baut derzeit seine Infrastruktur aus und wird damit nach eigenen Angaben zum weltweit größten Peering-Knotenpunkt für Internetprovider. Die bisher installierte Kapazität von 350 Gbit/s reichte bereits für Rang zwei. Die Umstellung auf eine sternförmige Topologie soll Mitte Juni abgeschlossen sein und dem DE-CIX einen Datenumsatz von 1,4 Tbit/s ermöglichen. Laut Betreiberin, der DE-CIX Management GmbH, erfordert besonders das starke Wachstum des osteuropäischen Breitband-Markts einen Ausbau. So habe sich der Internet-Verkehr bei DE-CIX im vergangen Jahr verdreifacht, während er sich weltweit im selben Zeitraum „nur“ verdoppelte.

Aufgebohrt: Das Linux Professional Institute (LPI, www.lpi.org) arbeitet an einer Security-Prüfung als Erweiterung des „Enterprise Level“ (LPIC3) seiner Linux-Zertifizierungsserie. Nach derzeitiger Planung sollen Bewerber ab Ende Februar 2009 die Prüfung „Security“ (LPI-303) ablegen können.

RFID-Umfrage: Noch bis zum 25. April haben Interessierte die Möglichkeit, zu einem Empfehlungsentwurf für den EU-Rat und das Parlament Stellung zu nehmen. Themen sind vor allem Datenschutz sowie Risiken für Privatsphäre und Sicherheit im Zusammenhang mit RFID. Da mit der Annahme des Entwurfs im Sommer 2008 zu rechnen ist, ruft der in Sachen Datenschutz engagierte Verein Foebud zur Teilnahme an der öffentlichen Kommentierung auf (erreichbar via *iX*-Link).

iX0805020

Schadensersatz nach Datenschutzgesetz

Obwohl ein Österreicher Widerspruch gegen eine fälschlicherweise zugesandte Rechnung über 100 Euro eingelegt hatte, listete ihn der Rechnungssteller in einer Bonitätsdatenbank. Daraufhin wurde ihm der Abschluss eines Mobilfunkvertrages verwehrt. Das Landesgericht für Zivilsachen in Wien (Az. 53 Cg 106/07h) hat dem Betroffenen nun Schadensersatz in Höhe von 750 Euro zugesprochen. Damit gab es erstmalig immateriellen Schadensersatz nach dem österreichischen Datenschutzgesetz 2000. Hierauf hat Hans Zeger, Vorstand der österreichischen Gesellschaft für Datenschutz, hingewiesen.

Tobias Haar

Google buhlt um Webentwickler

Unter dem Namen App Engine öffnet Google die eigene Server-Infrastruktur und Entwicklungsumgebung. Programmierer können zukünftig den neuen Service zum Hosten eigener Applikationen nutzen. Sie müssen sich im Grunde nur festlegen, welche URLs genutzt werden, mit welchen Programmen sie verbunden sind und im Anschluss ihre Anwendung aufspielen. Das Zuordnen von Ressourcen, Skalieren oder die Lastverteilung soll App Engine übernehmen. Der Service umfasst unter anderem einen Datenspeicher einschließlich Abfrageumgebung und Transaktionsverarbeitung sowie Anwendungsschnittstellen zur Authentifizierung der Anwender und zum E-Mail-Versand über Google-Accounts. Des Weiteren gibt es eine lokale Entwicklungsumgebung, die App Engine auf dem eigenen System simuliert.

Derzeit unterstützt App Engine allein eine Betriebsumgebung, die auf der Skriptsprache Python (Version 2.5.2) beruht. Es steht hier zwar im Prinzip die Standardbibliothek einschließlich eines einfachen Web Application Framework (Webapp) bereit. Die Entwickler müssen allerdings mit einigen Einschränkungen leben. So sind einige Module der Python-Standardbibliothek unbrauchbar, da die Laufzeitumgebung sie nicht unterstützt. Programme, die diese Module nutzen, verursachen deshalb ebenso eine Fehlermeldung wie Anwendungen mit Bestandteilen in C. Sorgfalt erfordert ebenso das in App Engine enthaltene Web Application Framework Django (Version 0.96.1). Denn manche Komponenten setzen hier eine relationale Datenbank voraus, die App Engines Datastore nun einmal nicht bietet. Wie lange Entwickler mit diesen Beschränkungen leben müssen, ist nicht bekannt. Zumindest verspricht Google, künftig weitere Programmiersprachen und Runtime-Konfigurationen unterstützen zu wollen.

Google ist mit der Öffnung der Entwicklungsumgebungen und -dienste über das Web für die Allgemeinheit nicht alleine im Markt. Anders als konkurrierende Angebote etwa von Amazon und Salesforce soll die App Engine in der Basisversion allerdings gratis sein. Sie umfasst 500 MByte Speicherplatz, 10 GByte an täglichem Traffic und genug Rechenleistung für 5 Mio. Page Views pro Monat. Details zu kostenpflichtigen Versionen gibt es derzeit nicht. Die zum Start von App Engine bereitgestellten 10 000 freien Accounts sind bereits belegt. Weitere Interessenten kommen auf eine Warteliste.

Über das Motiv von Google, die eigenen Ressourcen freizugeben, gibt es derzeit heftige Spekulationen. Für einige Marktbeobachter ist es einfach der Versuch, die Werbeprogramme Adsense und Adwords auf eine noch breitere Basis zu stellen. Andere erkennen eher das Bemühen, auf diese Weise sehr viel schneller Innovationen im Webmarkt erkennen, aufkaufen und schließlich aufgrund der gemeinsamen Entwicklungsumgebung auf einfache Weise in das eigene Angebot integrieren zu können. Auf diese Weise ließe sich zumindest indirekt ein wenig des Start-up-Geistes zurückgewinnen, der Google einst auszeichnete.

Achim Born

Datenschützer fordern Respekt vor Grundrechten

„Wir brauchen eine neue Datenschutzkultur“ forderte Peter Schaar anlässlich der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Denn Regelungen zum Großen Lauschangriff, zur Telekommunikationsüberwachung, zur Onlinedurchsuchung et cetera, so der Bundesdatenschutzbeauftragte weiter, „haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet“. Das Bundesverfassungsgericht habe mit seinen Entscheidungen diese Balance wiederhergestellt und den Forderungen der Datenschützer Rechnung getragen.

Die Konferenz befasste sich unter anderem mit den Auswirkungen des BVerfG-Urteils zu heimlichen Onlinedurchsuchungen. Das gerichtlich festgestellte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nehme auch den Staat in die Verantwortung, sich aktiv dafür einzusetzen und Bürgerinnen und Bürger vor „elektronischer Ausforschung“ zu schützen, so die Datenschützer.

Kurz vor der Konferenz hatte der Berliner Datenschutzbeauftragte seinen Jahresbericht veröffentlicht. Der Einsatz des Internet, so Alexander Dix, „muss aus gutem Grund anonym und unbeobachtbar möglich sein“, denn die ungehinderte Nutzung von Webangeboten sei Bestandteil einer freiheitlichen Gesellschaft. Weitere Themen sind Voice over IP, biometrische Authentifizierung, Datenschutz bei Berliner Banken und der von Datenschützern mit Argwohn betrachteten Entwurf zur Änderung des BKA-Gesetzes. Der Bericht und alle Veröffentlichungen zur Datenschutzkonferenz sind via *iX*-Link online abzurufen.



10GE-Adapter für Twisted-Pair-Kabel

SMC (www.smc.de) hat den nach eigenen Angaben ersten Ethernet-Adapter für 10GE über Twisted-Pair-Kabel (10GBase-T) auf den Markt gebracht. Der SMC10GPCIe-10BT genügt dem IEEE-Standard 802.3an. Sein Vetter SMC10GPCIe-XFP arbeitet mit steckbaren XFP-Transceivern (10 Gigabit Small Form Factor Pluggable) für Kurz- (SR, bis 300 m) und Langstrecken (LR, bis 10 km).

Prüfsummengeneratoren und -checker sowie eine TCP Segmentation Offload (TSO) Engine entlasten die Prozessoren des Rechners. Virtualisierten Betriebssystemen stellen die Adapter bis zu 4096 virtuelle Netzwerkkarten (VNICs) bereit. Die PCIe-x8-Steckkarten sind für 1299 € (Twisted Pair) beziehungsweise 789 € (XFP-Version ohne Transceiver) erhältlich. Geeignete Treiber gibt es für Windows Server 2003/2008 und Vista, Opensolaris und Linux – Letztere auch als Quelltext.

Open Source bald überall

In der Vergangenheit fielen die Analysen von Gartner oft durch ihre kritische Haltung gegenüber freier Software auf. Jetzt befragten die Marktforscher über 50 Analysten diverser Industriebereiche zu ihrer Einschätzung über Open-Source-Software (OSS). Die Ergebnisse fasste man in vier Voraussagen für die kommenden Jahre zusammen. www.gartner.com/DisplayDocument?id=638643&ref=g_sitelink liefert weitere Details.

Bis 2011 werde OSS bei Cloud-Providern die Software-Infrastruktur dominieren. Diese würden in ihren Rechenzentren zur Kostenreduzierung in Eigenverantwortung gepflegte, das heißt, ohne auf kommerzielle Angebote großer Distributoren zuzugreifen, Linux-Umgebungen einsetzen und so die Lizenzkosten eliminieren.

Bis 2012 würden auch die SaaS-Anbieter auf den Einsatz von OSS als bevorzugte Methode zur Kostensenkung umschwenken. Zum einen sei der SaaS- ebenso wie der OSS-Markt ein Segment mit kleinen Margen, und zum anderen würden sich die Provider mit OSS die nötige Unabhängigkeit sichern, um schnell auf Veränderungen reagieren zu können. Auch die dritte Vorhersage betrifft 2012: In diesem Jahr werden über 90 % aller Unternehmen OSS einsetzen – entweder direkt oder in eingebetteter Form. Mit dieser Ansage zollt Gartner dem OSS-Boom im Embedded-Bereich Respekt.

Schließlich prophezeien die Marktforscher, dass für den Großteil der Linux-Lösungen die TCO-Vorteile bis 2013 faktisch auf Null sinken werden. Das liege unter anderem daran, dass mit der Professionalisierung und dem Wachstum der IT-Umgebungen der Anteil von Anwendungen wie Datenbanken, Systemmanagement-Tools oder Hochverfügbarkeitssoftware zulegen werde, die aber wie heute überwiegend proprietär lizenziert würden.

Wer den Linux-Code schrieb

In akribischer Arbeit haben Kernel-Entwickler Greg Kroah-Hartman von den Suse Labs, LWN-Redakteur Jonathan Corbet und Amanda McPherson von der Linux Foundation die Veränderungen am Linux-Kernel von Version 2.6.11 bis zu 2.6.24 untersucht und analysiert, wer in welchem Umfang zum Linux-Kernel beigetragen hat. Bei inzwischen fast neun Millionen Zeilen (2.6.24) Code fließen in den rund 80 Tagen von einer zur nächsten Release knapp 10 000 Patches in die Kernel-Quellen ein. Im betrachteten Zeitraum haben fast 3700 Entwickler eine oder mehrere Änderungen beigetragen. Die Ergebnisse widerlegen – zumindest für den Kernel – den Mythos, Linux sei ein von Hobbyisten getragenes Projekt. Nur rund ein Viertel der Änderungen stammen von unabhängigen Programmierern, der Rest arbeitet bei Firmen an der Linux-Entwicklung mit. Bei den firmenbezogenen Anteilen liegt Red Hat mit 11,2 % vorn, gefolgt von Novell (8,9 %), IBM (8,3 %) und Intel (4,1 %).

Detaillierte Ergebnisse der Untersuchung finden sich unter www.linux-foundation.org/publications/linuxkerneldevelopment.php. Die Linux Foundation ist Anfang 2007 aus einer Fusion der Free Standards Group und den Open Source Development Labs hervorgegangen und unter anderem Brötchengeber von Linus Torvalds und einer Reihe weiterer Kernel-Entwickler.

KURZ NOTIERT



Wartungs-Release: Die Verbesserungen der jetzt veröffentlichten KDE-Version 4.0.3 betreffen neben vielen Polierarbeiten die KDE-HTML-Rendering-Engine KHTML, den Window-Manager KWin sowie den Dokumentenbetrachter Okular. Darüber hinaus verschafft ein KIO-Plug-in aus den Extragear-Paketen allen KDE-Anwendungen Unterstützung für das Gopher-Protokoll.

Großstädte sind lukrative Standorte

Arbeitsort und Branche beeinflussen in entscheidendem Maß die Höhe der Vergütung. Zu dieser nicht neuen Erkenntnis kommt eine Untersuchung der Gummersbacher Unternehmensberatung Kienbaum. Beispielsweise verdient ein Münchner Ingenieur in einer Führungsposition durchschnittlich 117 800 Euro im Jahr, während Berufskollegen in Leipzig lediglich auf 70 300 Euro kommen. Tendenziell werden in Großstädten und Ballungszentren wie München, Düsseldorf, Frankfurt/Main und Köln die höchsten Gehälter gezahlt. Im ländlichen Raum und in Ostdeutschland fällt die Vergütung am geringsten aus. IT-Führungskräfte verdienen wiederum in Nordrhein-Westfalen am besten. Eine Führungskraft aus Düsseldorf (Jahresgesamtbezüge: 131 000 Euro) hat in der Regel ein Viertel mehr im Portemonnaie als der Durchschnitt. Ein Kölner IT-Spezialist (121 000 Euro) streicht über 15 % mehr Gehalt ein.

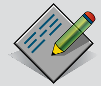
IT-Fachkräfte: Mangel allerorten

Fehlende IT-Spezialisten sind kein ausschließlich deutsches Phänomen, so die Einwanderungsbehörde Immigration New Zealand und der Personaldienstleister Hudson Recruitment auf der diesjährigen Cebit. Arbeitsbedingungen und Verdienstmöglichkeiten in Neuseeland sind durchaus konkurrenzfähig. Das Gehaltsniveau für Java-Programmierer beträgt laut Hudson-Statistik pro Jahr zwischen 55 000 NZD (neuseeländische Dollar, ungefähr 0,50 €) für einen Juniorentwickler und 140 000 NZD für einen J2EE-Architekten. Oracle-Administratoren streichen je nach Erfahrung zwischen 65 000 NZD und 120 000 NZD ein. Projekt-Manager verdienen zwischen 80 000 NZD und 125 000 NZD. Wer zwischen 18 und 30 Jahre ist, kann im Rahmen des Working Holiday-Programms erste Eindrücke zum Arbeiten und Leben am anderen Ende der Welt gewinnen. Unter www.immigration.govt.nz gibt es nähere Informationen zu diesem Programm und zu den Einwanderungsbedingungen allgemein.

IGM rät, Arbeitsverträge zu prüfen

Die IG Metall empfiehlt Berufsanfängern, genau auf die Gehaltsdetails wie Anzahl der Monatsgehälter, Arbeitszeit und Zulagen zu achten. Laut Gewerkschaftsstatistik liegen Einstiegsgehälter innerhalb einer großen Bandbreite. Beispielsweise kann das Salär für einen Informatiker mit Diplom- oder Masterabschluss zwischen 39 000 Euro und 50 300 Euro betragen. Mit 33 500 Euro und 47 500 Euro fällt die Spreizung für Absolventen von Bachelor-Studiengängen noch größer aus. Absolventen von Fachhochschulen erhalten zwischen 38 300 Euro und 42 000 Euro.

KURZ NOTIERT



Mangel: Die Hälfte der im VDE organisierten Unternehmen befürchtet einen anhaltenden Mangel an Elektro- und IT-Ingenieuren. Die circa 9600 Hochschulabsolventen der Elektrotechnik werden nach Ansicht von Verbandsvertretern den Fachkräfte-Bedarf der deutschen Wirtschaft nicht annähernd decken können. Auch in Forschung und Lehre soll der Nachwuchsmangel mittlerweile zu spüren sein.

Studiengang: In Bremen wurde der Bachelor-Studiengang Informationstechnische Systeme (BITS) gegründet. Der Studiengang befasst sich mit den informationstechnischen Aspekten der Elektrotechnik und löst den Studienschwerpunkt IT des bisherigen Diplom-Studienganges Elektrotechnik ab. Bewerbungsschluss ist der 15. Juli.

Erste Barcelona-Server in Sicht

Spanischer Reigen

Susanne Nolte

„Erster!“ konnte diesmal HP rufen: Auf der „HP Technology@Work 2008“ in Barcelona hatte Hewlett-Packard mit dem Proliant DL785 G5 den ersten 8-Sockel-Server mit fehlerfreien Opteron-Quad-Core-Prozessoren (Barcelona) vorgestellt. Andere Hersteller hingegen lassen sich noch Zeit.

Nachdem ein Bug im TLB (Translation Lookaside Buffer) die Opteron-Serienproduktion bei AMD über Monate verzögert hat, sollen die CPUs im fehlerbereinigten B3-Stepping im Mai in größeren Stückzahlen verfügbar sein.

Nun traut sich HP als Erster, seine neue Servergeneration mit den Quad-Core-CPUs von AMD anzukündigen. Das Flaggschiff bildet der Acht-Sockel-Server für Opteron-CPUs der 8300er-Serie. Als einziges Modell nennt HP momentan den Opteron 8354 mit 2,2 GHz. Mit den derzeitigen 4-GByte-DDR2-RAM-Modulen kommt man auf bis zu 256 GByte, mit den noch ausstehenden 8-GByte-DIMMs auf 512 GByte Hauptspeicher. Die Festplattenkapazität beträgt bei 16 SAS-Festplatten (8 Standard und 8 optional) maximal 2,3 TByte. Da HP den Server besonders zum Einsatz in Virtualisierungsumgebungen anbietet, sind 11 PCIe-Steckplätze vorgesehen. Auf das zweite Halbjahr müssen diejenigen warten, die statt der elf PCIe-Slots sieben PCIe- und zwei HTx-Steckplätze haben wollen.

HP goes Solaris

Zertifiziert ist das System für Microsoft Virtual Server, Oracle VM und VMware ESX; es unterstützt die Betriebssysteme RHEL, SLES, Windows 2003 Server und Solaris. Letzteres will HP in Zukunft intensiver bewerben, da der Hersteller verstärkt in Suns Revieren wildern will. Der DL785 kommt serienmäßig mit den schon von anderen Proliant-Servern bekannten Managementwerkzeugen HP Systems Insight Manager, HP Insight Control, HP Integrated Lights Out 2 (ILO 2) und HP Proliant Essentials.

Proliant DL585 G5 heißt das 4-U-System mit vier Opteron 8354 oder 8356 (2,3 GHz), 4 bis 128 GByte Hauptspeicher, bis zu acht 2,5"-SAS- oder -SATA-Platten im RAID-Verbund, zweimal Gigabit Ethernet mit TOE (TCP/IP Offload Engine), sieben PCIe- und zwei PCI-X-Slots sowie Integrated Lights Out 2 für das Remote-Management. Sein Preis beginnt bei 8792 US-Dollar.

Hinter der Bezeichnung Proliant DL185 G5 verbirgt sich ein Server im 2-U-Chassis mit zwei Opteron 2352 (2,1 GHz), 1 bis 32 GByte RAM, maximal 14 3,5"-Festplatten und Dual-Gigabit-Ethernet. Er kostet 1749 US-Dollar aufwärts. Das zweite 2-U-System Proliant DL385 G5 ist dagegen mit zwei Opteron 2352 oder 2356 (2,3 GHz), 2 bis 32 GByte Arbeitsspeicher und bis zu acht 2,5"-SAS- oder -SATA-Platten im RAID-Verbund, zwei Gigabit Ethernet mit TOE, PCIe, optional PCI-X, und ILO 2 ausgestattet. Sein Preis beginnt bei 2379 US-Dollar.

In der 1-U-Klasse bietet HP die Zwei-Sockel-Systeme Proliant DL165 G5 und DL365 G5 auf; Ersteren bestückt mit zwei Opteron 2352 oder 2356, 2 bis 32 GByte RAM und bis zu vier SAS- oder SATA-Laufwerke im 3,5"-Format. Hinzu gesellen sich 2 × Gigabit Ethernet und Lights Out 100i; Preis: ab 1479 US-Dollar. Der Proliant DL365 G5 ist nur mit den Opteron-Modellen 2352 oder 2354 (2,2 GHz), dafür jedoch mit bis zu sechs 2,5"-SAS- oder -SATA-Platten und ILO 2 ausgestattet. Der Preis beginnt bei 1799 US-Dollar.

Die Barcelona-Blades nennt HP Proliant BL465c G5 und BL685c G5. Erstere arbeitet mit zwei Opteron 2352, 2354 oder 2356 und 2 bis 32 GByte Arbeitsspeicher und maximal zwei 2,5"-SAS- oder -SATA-Platten im RAID-Verbund, zwei Gigabit Ethernet und Management-Port für ILO2. Der Preis beginnt bei 2519 US-Dollar. Die BL685c G5 rechnet dagegen mit vier Opteron 8354 (2,2 GHz) oder 8356 (2,3 GHz) und kann 8 bis 64 GByte RAM aufnehmen. Zudem führen vier GE-Ports nach draußen. Dafür kostet sie auch mindestens 10 649 US-Dollar.

Derweil halten sich die Mitbewerber Dell, Fujitsu-Siemens, IBM und Sun mit konkreten Ankündigungen zurück. Als Erster wird wohl IBM nachziehen.

Atempo kündigt neue Archivsoftware an

Seiner Archivierungslösung für mittelständische und große Unternehmen, Archive Server, hat Atempo (www.atempo.com) nicht nur den neuen Namen Atempo Digital Archive (ADA) 2.0, sondern auch einige neue Funktionen spendiert. Darunter eine Daten-Deduplizierung, die den Speicherbedarf verringert. Außerdem erlaubt es die neue Version, die gespeicherten Dokumente vollständig zu katalogisieren. Umfangreiche Suchfunktionen sollen das Abrufen von Daten vereinfachen.

Zum Lieferumfang gehört außerdem ein „Atempo-Meter“ genanntes Werkzeug, das den Online-Datenbestand überprüft sowie ungenutzte und daher archivierbare Dateien anzeigt. Verschiebt man sie regelmäßig auf günstigere Speichermedien wie SATA-II-Festplatten, Magnetbänder oder optische Medien, kann man die Kosten deutlich reduzieren.

Ab Mitte April soll die Software für Linux, Mac OS X, diverse kommerzielle Unix-Varianten – darunter AIX, HP-UX und Solaris – sowie Windows erhältlich sein. Die Preise sind volumenabhängig; der Einstiegspreis liegt bei 8000 € für 1 TByte Kapazität.

256 GByte große Flash-SSD für Notebooks

Der US-amerikanische Speicherhersteller Super Talent (www.supertalent.com) liefert Muster einer 256 GByte großen Solid State Disk (SSD) an OEMs. Das 2,5-Zoll-Modell FSD56GC25H besitzt eine mittlere Zugriffszeit von nur 0,1 Millisekunden, liest und schreibt mit 65 beziehungsweise 50 MByte/s schneller als die meisten Festplatten der gleichen Bauform und schließt auch in puncto Kapazität zu seinen mechanischen Vettern auf. Allerdings passt das 12,5 mm dicke SATA-Laufwerk nicht in jedes Gerät.

Sehen lassen können sich auch die Angaben zu Verlässlichkeit und Haltbarkeit. Erstere beziffert der Hersteller mit einer MTBF (Mean Time Between Failures) von über 1000 000 Stunden, entsprechend einer Annual Failure Rate (AFR) von 0,88 %. Ein patentierter Wear-Leveling-Algorithmus soll verhindern, dass die Flash-Speicherzellen vorzeitig altern: Laut Super Talent leben sie länger als 140 Jahre, wenn man jeden Tag 50 GByte schreibt – bei größerem Datenaufkommen entsprechend kürzer. Keine Angaben macht der Hersteller hingegen zum Energiebedarf. Preise gibt die Firma auf Anfrage bekannt.

Viel Neues aus dem Hause Adobe

Diverse Neuigkeiten gibt es aus dem Hause Adobe. AIR, die bisher nur für Mac- und Windows-Plattform verfügbare Desktop-Laufzeitumgebung für Webanwendungen, liegt jetzt als Alpha-Version auch für die Linux-Plattform vor (www.adobe.com/go/airlinux). AIR unterstützt Webtechniken und Sprachen wie HTML, Javascript Ajax oder DOM. Für die Entwicklung von Rich Internet Applications (RIAs) lässt sich der hauseigene Flex Builder nutzen, für den ebenfalls eine Alpha-Version für Linux zum Download bereitsteht (www.adobe.com/go/flex builder_linux). Adobes Beitritt zur Linux Foundation lässt annehmen, dass der Hersteller die Entwicklung der Linux-Versionen weiterhin vorantreiben wird.

Zur Version 8 des Web Applications Server Coldfusion, der ersten Major Release seit der Übernahme von Macromedia durch Adobe, bietet der Hersteller unter www.adobe.com/support/coldfusion/down loads_updates.html Updater an. Der bisherige Support von 64 Bit unter Solaris wurde ausgeweitet auf Windows-, Linux- und Macintosh-Plattformen. Unterstützt werden jetzt außerdem Windows Server 2008 und Mac OS X 10.5.

Ein Lizenzabkommen mit Microsoft soll dafür sorgen, dass die Lite-Version des Flash Player demnächst über Mobiltelefone mit Microsofts Windows Mobile Zugriff auf interaktive Web-Inhalte erlaubt, die auf Flash-Basis erstellt wurden. Analog dazu soll die Lizenzierung von Adobes Reader LE die Anzeige von PDF-Dokumenten auf Windows-Handys erlauben.

Als kostenlose Onlinesoftware bietet Adobe die Public Beta von Photoshop Express an (www.photoshop.com/ex press). Die auf Flex basierende Anwendung lässt sich aus einem beliebigen Webbrowser heraus aufrufen, vorausgesetzt, ein Flash Player 9 ist installiert. Nutzer können Fotos bis zu einem Volumen von 2 GByte speichern und online bearbeiten – beispielsweise rote Augen entfernen oder Bildbeschneidungen oder Größenanpassungen vornehmen. Adobe bietet sich als Webhoster für die Veröffentlichung von Fotos und Diashows an, es ist aber auch möglich, die Bilder in persönliche Blogs oder Social-Networking-Seiten wie Facebook einzubinden.

Debugging mit dem Flash Development Tool

Wie schon angekündigt bietet die Aachener Powerflasher GmbH jetzt auch die Enterprise Edition von FDT 3.0 an (fdt.powerflasher.com). Das Eclipse-Plug-ins stellt eine IDE für Flash und Actionscript zur Verfügung . Im Vergleich zu den Basic- und Professional-Versionen zeichnet sich die Enterprise-Variante vor allem durch einen Debugger aus. Durch die Nutzung der Debug-Perspektive von Eclipse können Anwender wie im Flex Builder oder in den Java Development Tools (JDT) Fehler suchen und beheben. Als Preis für die Vollversion des Flash Development Tool nennt der Hersteller 599 €, ein Upgrade kostet 100 Euro weniger.

Quark unterstützt Microsofts Silverlight

In seinem Technologieportal Quark Labs (labs.quark.com) bietet der Hersteller der Desktop-Publishing-Software seinen Kunden die Möglichkeit, neue Erweiterungen zu testen, die noch nicht im Handel erhältlich sind. Dazu zählt unter anderem das Modul Quarkviewer XT für QuarkXpress 7, das Microsofts Silverlight unterstützt. Silverlight bietet eine Alternative zu Flash für das Abspielen multimedialer Inhalte im Web sowie die Wiedergabe von Rich Internet Applications (RIAs). Mit dem Silverlight-Plug-in können Benutzer von QuarkXpress 7, die unter Windows arbeiten, komplexe interaktive Dokumente für das Internet direkt aus der Publishing-Software heraus generieren.

Programmierer haben Namensnennungsrecht bei eigener Software

Das Oberlandesgericht Hamm (Urteil vom 7. August 2007, Az. 4 U 14/07) hat einem Programmierer ein Namensnennungsrecht auch dann zugesprochen, wenn dieser einem anderen ein umfassendes und ausschließliches Nutzungs- und Verwertungsrecht an seinen Programmierleistungen eingeräumt hat. Die Richter begründen dies mit dem Urheberpersönlichkeitsrecht. Der Beklagte wurde deswegen verurteilt, weil er Hinweise auf den Programmierer unter anderem im Copyright-Vermerk weggelassen hatte.

Die Richter geben Urhebern durchaus das Recht, vertraglich auf dieses Namensnennungsrecht zu verzichten. Allerdings muss ein solcher Verzicht in der Regel ausdrücklich erfolgen.

Liegt dieser Verzicht nicht vor oder gibt es daran Zweifel, hat der Programmierer trotz weitreichender Rechtseinräumung darauf nicht verzichtet und kann weiterhin entsprechende Ansprüche geltend machen.

Um Ärger zu vermeiden, müssen Urheber und Erwerber von Nutzungsrechten also unbedingt darauf achten, dass sie auch diese Punkte eindeutig in den jeweiligen Lizenzverträgen regeln. *Tobias Haar*

BGH: Keine umfassende Vorratsdatenspeicherung

Nach dem im März verkündeten Beschluss des Bundesverfassungsgerichts (BVerfG vom 19.03.2008, Az. 1 BvR 256/08) zur umstrittenen Vorratsdatenspeicherung gab es augenscheinlich nur Sieger. Während die Gegner mit Presseerklärungen wie „Karlsruhe schränkt Vorratsdatenspeicherung ein“ aufwarteten, erklärte das Bundesjustizministerium eilig „Vorratsdatenspeicherung bleibt zulässig“. Wie ist das möglich? Tatsächlich hat das Bundesverfassungsgericht beiden Seiten Recht gegeben. Genauso gut könnte man sagen, beide Seiten haben teilweise verloren. Noch aber ist das Thema nicht endgültig vom Tisch, denn das Gericht hat zunächst nur in einem Eilverfahren entschieden. Das bedeutet, dass diese Entscheidung nur eine vorläufige ist. Trotzdem ist sie bemerkenswert, denn normalerweise hält sich das Gericht in solchen Eilsachen sehr zurück.

In der Vorratsdatenspeicherung „liegt ein schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Artikel 10 Abs. 1 GG (Schutz des Telekommunikationsgeheimnisses)“, so die Karlsruher Richter. Und weiter: „Ein solcher Datenabruf ermöglicht es, weitreichende Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte des Betroffenen zu erlangen.“ Aber sie entschieden auch, dass die Vorratsdatenspeicherung an sich zunächst zulässig bleibt. Zunächst bedeutet, bis die Verfassungsbeschwerden in der Hauptsache entschieden werden. Bis dahin aber ist die Nutzung der gespeicherten Daten beschränkt. Sie dürfen nur zur Verfolgung „schwerer Straftaten“ verwendet werden. Was für Straftaten das sind, definiert § 100a der Strafprozessordnung. Hierzu zählen neben Kapitalverbrechen wie Mord, Totschlag und Raub Vergehen wie Betrug, Bestechung, Geldwäsche et cetera. Es handelt sich um diejenigen Straftaten, für die die Befugten auch bislang schon die Überwachung von Telefonaten einer verdächtigen Person anordnen können.

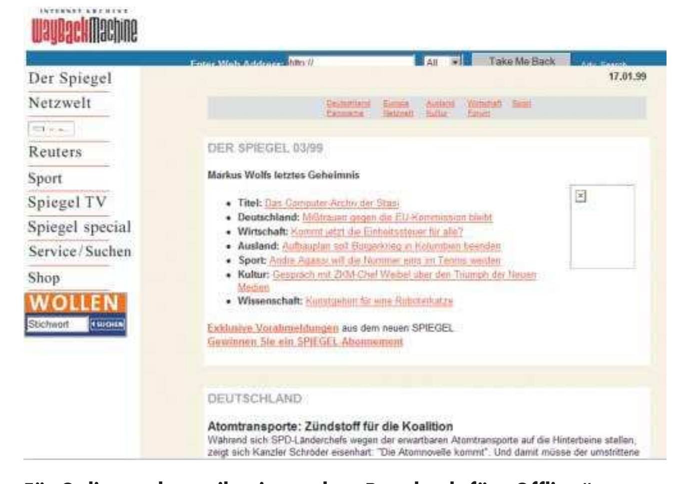
Auf einen wesentlichen Aspekt dieser vorläufigen Entscheidung hat der Verband der deutschen Internetwirtschaft (eco) hingewiesen. Die im Rahmen der Vorratsdatenspeicherung erfassten Daten dürfen nicht zur Aufklärung von Urheberrechtsverletzungen verwendet werden, da es sich hierbei gerade nicht um schwere Straftaten handelt. Damit könnte das Bundesverfassungsgericht auch schon einen Hinweis gegeben haben, wie es eine geforderte Gesetzesänderung zur Einführung einer Pflicht der Internet-Access-Provider bewerten würde, bei Urheberrechtsverstößen Daten über ihre Kunden an die Musikindustrie herauszugeben.

Eine erste Konsequenz aus der Gerichtsentscheidung dürfte die Entscheidung der Staatsanwaltschaft Düsseldorf sein, Strafanträge der Musikindustrie nicht mehr zu bearbeiten. In diesen wird meist unter Nennung einer IP-Adresse eine Urheberrechtsverletzung angezeigt. Bislang ermittelte die Staatsanwaltschaft in solchen Fällen über die Access-Provider den Nutzer der genannten IP-Adresse, gegen den der Antragsteller dann Schadenersatzansprüche geltend machen konnte. *Tobias Haar*

Kein „Archiv-Privileg“ für Onlinearchive

Die Nennung eines wegen eines schweren Verbrechens Verurteilten beim Namen in einem Presseartikel kann zulässig sein, um das berechtigte Informationsbedürfnis der Öffentlichkeit zu befriedigen. Eine Weile nach der Veröffentlichung eines solchen Artikels kann allerdings seine Löschung angebracht sein, um etwa die Resozialisierung des Straftäters nicht unnötig zu gefährden. Dann überwiegt das Persönlichkeitsrecht des Täters. Hiervon gibt es aber eine bedeutende Ausnahme. Nach dem von vielen Juristen vertretenen Archiv-Privileg bleibt auch in solchen Fällen eine Speicherung eines ursprünglich zulässigen und jetzt zu löschenden Artikels in einem Archiv legitim.

Das Landgericht Hamburg (Urteil vom 18. Januar 2008, Az. 324 O 507/07) hat nun aber entschieden, dass dieses Privileg nicht für Onlinearchive gilt. Die Richter sind der Auffassung, dass sich ein Onlinearchiv von einem „Offlinearchiv“ dadurch unterscheidet, dass auf Ersteres jederzeit eine fast beliebige Nutzerzahl zugreifen kann. Beim Offlinearchiv kommt es nur dann zu einem Zugriff, wenn ein Interessent nach dem Artikel „archivarisch“ sucht. Das Onlinearchiv führt also zu einer wesentlich intensiveren Belastung des Betroffenen in solchen Fällen. Bereits 1966 hat der Bundesgerichtshof entschieden, dass „der technische Fortschritt, der die Speicherung und Zugänglichmachung von Daten in immer weiterem Umfang zulässt (…), nicht dazu führen (darf), dass Persönlichkeitsrechtsverletzungen eher hinzunehmen sind“. Das Urteil lässt sich auch auf Urheberrechtsverletzungen übertragen. Ein Onlinearchiv darf eine einmal legal erstellte Kopie eines urheberrechtlich geschützten Werkes nicht ohne Weiteres jedem zugänglich machen, wenn später das Nutzungsrecht erloschen ist. Ein Offlinearchiv nach dem Urheberrechtsgesetz aber schon. *Tobias Haar*



Für Online- gelten teilweise andere Regeln als für „Offline“-Archive, denn durch die leichte Verfügbarkeit für große Nutzerzahlen ist ein besserer Schutz der Persönlichkeitsrechte nötig.

Adwords-Urteil

Das Oberlandesgericht Frankfurt (Main) hat entschieden (Beschluss vom 26. Februar 2008, Az. 3/11 O 16/08), dass die Nutzung von Google-Ads keine wettbewerbsrechtlich unzulässige Rufausbeutung nach dem Gesetz gegen den unlauteren Wettbewerb darstellt. Im Gegensatz zu Metatags führen Google-Ads nur zu einer bestimmten Platzierung einer Werbeanzeige. Dies genügt aber noch nicht, um darin auch eine „kennzeichenrechtliche Benutzungshandlung“ zu sehen, die für einen Wettbewerbsverstoß erforderlich ist.

Anders ist der Fall nur dann zu bewerten, wenn die durch das Keyword aufgerufene Werbeanzeige nicht als solche klar und eindeutig erkennbar ist und nicht von der Trefferliste getrennt dargestellt wird. Die Richter distanzieren sich damit deutlich von einer Gleichsetzung von Adwords mit Metatags bei deren rechtlicher Bewertung, wie dies durch andere Gerichte in der Vergangenheit teilweise erfolgt ist.

Tobias Haar

Sammler von IP-Adressen verklagt

Der Schweizer Datenschutzbeauftragte Hanspeter Thür geht gerichtlich gegen ein Unternehmen vor, das sich heimlich IP-Adressen von Internetnutzern beschafft, die mutmaßliche Urheberrechtsverletzungen in Filesharing-Systemen begangen haben. Dieses Sammeln erfolgt mit einer speziellen Software. Nachdem der Datenschutzbeauftragte das betroffene Unternehmen darauf hingewiesen hat, dass dieses Vorgehen gegen das schweizerische Datenschutzrecht verstößt, verklagte er das Unternehmen nun. Dieses hatte das beanstandete Verhalten nicht eingestellt, weil es den Datenschutzbeauftragten für solche „Abmahnungen“ für nicht zuständig hält.

Angeblich waren insbesondere deutsche Unternehmen Abnehmer der IP-Adressen den schweizerischen Adressensammlers. Mit diesen Informationen wurden Strafanzeigen gegen die IP-Nutzer gestellt.

Tobias Haar

Neue offizelle Widerrufsbelehrung für den Fernabsatz

Seit 1. April 2008 gilt für Fernabsatzverträge eine neue Widerrufsbelehrung. Damit reagiert die Bundesregierung auf zahlreiche Gerichtsurteile, in denen die bislang gültige Widerrufsbelehrung als unwirksam eingestuft wurde. Einige Unternehmer waren abgemahnt worden, obwohl sie einen offiziellen Text verwendet hatten. Grund dafür war, dass dieser Text nicht mit der Gesetzeslage zum Widerruf von Fernabsatzverträgen durch Verbraucher im Einklang stand.

Problematisch war auch, dass die Widerrufsbelehrung, deren Verwendung übrigens nicht zwingend ist, nur als Verordnung und nicht als Gesetz erlassen wurde. Dies soll sich ebenfalls ändern und die Belehrung demnächst noch einmal in Gesetzesform verabschiedet werden. Den alten Text können Unternehmen noch bis zum 1. Oktober 2008 verwenden, den neuen finden sie unter www.bmj.de/bgbinfovo. *T. Haar*

Virenschutz mit neuen Features

Die Produkte des schwäbischen Herstellers Avira (www.avira.de) wurden in der neuen Version, der nun Aviras Scanengine 8.0 zugrunde liegt, gleich einer Namensänderung unterzogen. Sowohl Antivir Professional – vormals Antivir Workstation – als auch Antivir Premium – früher Antivir Personal Edition – verfügen über eine neue grafische Benutzeroberfläche. Diese ermöglicht laut Hersteller einen einfacheren und schnelleren Zugriff auf die einzelnen Module. Überdies kann man direkt aus der Oberfläche heraus Updates und Prüfdurchgänge starten.

Der Datendurchsatz beim Scannen soll um 20 % höher liegen als bei der Vorgängerversion. Neu in allen Versionen ist außerdem das integrierte Modul Webguard, das HTTP-Verkehr auf Malware untersucht und Phishing- sowie infizierte Websites automatisch blockiert.

Sicherheitslücken in Mifare-RFID-Chips

Mifare-Classic-Chips sind ins Gerede gekommen. Bereits Ende 2007 hat der Chaos Computer Club die Unsicherheiten des Systems beschrieben, und kürzlich bestätigte der Betreiber des landesweiten Bezahlsystems für den öffentlichen Nahverkehr, Trans Link Systems, die Unsicherheit.

In einer Stellungnahme räumt NXP Semiconductors ein, dass der Chip Mifare Classic ein schon seit 1995 auf dem Markt befindlicher „Mainstream-Chip“ sei, mit einer relativ schwachen Verschlüsselung. Im Einsatz sei er beim eTicketing im öffentlichen Nahverkehr und bei Zutrittskontrollsystemen, nicht aber auf E-Pässen, kontaktlosen Kredit- oder Debit-Karten oder sicherheitsrelevanten Auto-Anwendungen, betont der Halbleiter-Hersteller. Man nehme das Problem aber sehr ernst und sei mit den Experten vom Chaos-Computer-Club in einem offenen Dialog, beteuerte ein Sprecher von NXP gegenüber *iX*.

Bereits Ende 2007 habe man die Systemintegratoren benachrichtigt, mit der Empfehlung, die fraglichen Systeme genau zu untersuchen, um zu entscheiden, inwieweit Handlungsbedarf bestehe. Dabei sei aber eine Balance zwischen Kosten und dem tatsächlich benötigten Sicherheitslevel zu berücksichtigen. Darüber hinaus kündigte das Unternehmen den Chip „Mifare Plus“ für das vierte Quartal des Jahres an, was man aber nicht als Reaktion auf die Presseberichte verstanden wissen will. Mifare Plus unterstützt Verschlüsselung auf Basis des AES-Standards (Advanced Encryption Standard). Eine Migration von Mifare-Classic-Systemen auf Mifare Plus sei damit möglich. *Barbara Lange*

KURZ NOTIERT

Sichere Rücksendung: Ab sofort schickt der Forensik- und Datenrettungsdienstleister Kroll Ontrack (www.krollontrack.de) wiederhergestellte Daten in verschlüsselter Form an Kunden zurück. Verschlüsselt wird mit AES, den Entschlüsselungscode erhält der Kunde separat.

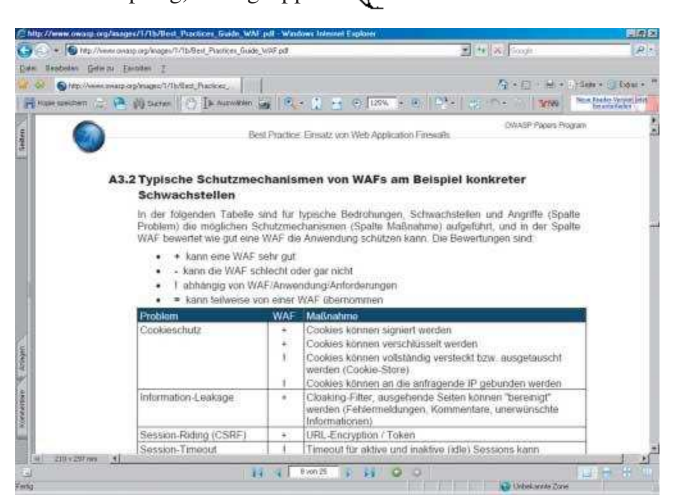
Gefahren-Report: Das seit einem Jahr existierende Storm-Botnet, das durch den gleichnamigen Wurm infizierte Rechner miteinander verbindet, war in den ersten drei Monaten dieses Jahres für 20 % des gesamten weltweiten Spam-Aufkommens verantwortlich, meldet der jüngste Quartalsbericht „Intelligence Report“ des Websicherheitsexperten MessageLabs. Er enthält zahlreiche Details zu Malware-Trends und sonstigen Webbedrohungen und ist online via *iX*-Link abzurufen.

iX0805028

Best Practices für Web Application Firewalls

Wenn Angriffe über erlaubte Kanäle kommen, etwa bei Webanwendungen über Formulare, helfen herkömmliche Firewalls wenig – Angriffen wie Cross-site Scripting oder SQL Injection kann man nur mit speziellen Web Application Firewalls (WAF) begegnen. Wie man diese am besten einsetzt, beschreibt ein neuer „Best Practice Guide“, herausgegeben von der im vergangenen Jahr gegründeten deutschen Sektion des Open Web Application Security Project (OWASP, www.owasp.org). Zielgruppe der 22-seitigen Broschüre sind technische Entscheider. Einer der Schwerpunkte befasst sich mit der Aufwandsabschätzung für das Installieren und Betreiben einer Web Application Firewall sowie für Alternativen wie das Anpassen des Sourcecodes. Weitere Themen betreffen die organisatorischen Prozesse bei Installation und Betrieb sowie die Einführung eines „Anwendungsverantwortlichen WAF“. Die Broschüre gibt es online, siehe *iX*-Link.

iX0805028



Die Auflistung der Schutzmöglichkeiten von Web Application Firewalls soll Entscheider bei der Einschätzung ihrer Wirtschaftlichkeit unterstützen.

Sicherheit 2008 – Jahrestagung der GfI

Sicherheit, Schutz und Zuverlässigkeit war auch in diesem Jahr das Motto der vierten Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik. Zur Konferenz „Sicherheit 2008“ in Saarbrücken kamen 150 IT-Sicherheitsexperten aus Wissenschaft, Industrie und dem öffentlichen Dienst. Kern des Tagungsprogramms bildeten durchweg qualitativ gute wissenschaftliche Beiträge zu den Themen Privacy Enhancing Technologies (PET), Kryptografie, Biometrie, Antispam und Antispit, Zuverlässigkeit von IT-Systemen sowie reaktive Sicherheit.

Konkret beleuchtete etwa ein Beitrag die Empfänger-Anonymität in Broadcast-Netzwerken anhand von Satellit- und Wide-Area-Netzwerken, ein weiterer die datenschutzrechtliche Aspekte unter anderem anhand des elektronischen Reisepasses. Auch die IT-Sicherheitsausbildung an deutschen Hochschulen war Thema. Ferner bot sich die Gelegenheit, innovative Anwendungsbeispiele aus der Industrie wie Smartcards mit SD-Interface oder ein Abwehrsystem für Spam-over-IP-Telephony (Spit) zu begutachten. Sehr interessante Einblicke in die Praxis von Einbruchstestern boten die Vorträge von Patrick Hof und Jens Liebchen von Redteam Pentesting – einem ausschließlich auf die aktive Überprüfung der Sicherheit von IT-Systemen spezialisierten Unternehmen. Die nächste Tagung findet voraussichtlich im Herbst 2010 in Kooperation mit der Information Security Solutions Europe (ISSE) in Darmstadt statt. *Christian J. Dietrich*

Windows Mobile 6.1 angekündigt

Version 6.1 von Microsofts Windows Mobile soll schneller auf SMS, E-Mails, unbeantwortete Anrufe und Unterhaltungsfunktionen zugreifen können. Der aktualisierte Browser verarbeitet Adobes Flash und Microsofts Silverlight sowie Videos im H.264-Format, verspricht der Hersteller. Außerdem soll ein Vollbildmodus den Abstand zur großen Version des Internet Explorer verringern.

Unternehmen verspricht Microsoft eine einfachere Verwaltung der Windows-Mobile-Geräte mit dem System Center Mobile Device Manager. Den neuen Browser sollen Gerätehersteller im dritten Quartal bekommen; erste Modelle mit Windows Mobile 6.1 könnten Ende des Jahres erscheinen.

Flexibler VPN-Client für Symbian

Mit ihrem VPN-Client will die Nürnberger NCP engineering GmbH (www.ncp.de) eine Lücke auf Symbian-Geräten füllen. Die Software läuft auf S60-Modellen, zu denen unter anderem die Nokia-Smartphones der E-Serie gehören. Dort ist zwar ein VPN-Client verfügbar, er funktioniert jedoch lediglich mit einem Gateway von Nokia ohne Klimmzüge.

Nach Herstellerangaben arbeitet seine VPN-Software mit vielen Gateways zusammen, unter anderem mit den freien IPSec-Versionen von OpenBSD, Freeswan und Openswan. Die Authentisierung per Preshared Keys (PSK) ist mit allen Gegenstellen möglich, mit den meisten lässt sich außerdem die Anmeldung per Zertifikat bewerkstelligen.

NCP bietet wie bei seinen Windows-Mobile-Clients zwei Versionen an: Ab April soll es die Enterprise-Variante geben, für die der Hersteller eine Serverkomponente zur zentralen Verwaltung und Integration ins Unternehmensnetzwerk anbietet. Erst im Juli will er die Entry-Version ohne diese zentralisierte Administration herausbringen. Die Clients kosten 99 und 69 € netto.

Vodafone senkt Datentarif

Einen Monat nach T-Mobile reduzierte Vodafone den Preis für die Daten-Flatrate „Mobile Connect Flat“ auf ebenfalls 30 € netto monatlich. Ganz „flat“ ist dieser Tarif allerdings nicht: Hat der Kunde 10 GByte im laufenden Monat übertragen, drosselt Vodafone wie T-Mobile die Verbindung. Statt der maximal 7,2 Mbps im UMTS-Netz stehen dann nur noch rund 60 kbps zur Verfügung. Wer auch im Ausland regelmäßig ins Web möchte, bekommt für weitere 17 € zwei internationale Websessions pro Monat. Dieser Zugang steht in 35 Ländern für jeweils 24 Stunden zur Verfügung – bei maximal 50 MByte Datenvolumen pro Sitzung. Die Mindestlaufzeit der bis Ende Juli befristeten Angebote beträgt zwei Jahre.

Symbian integriert SQLite

Ab dem zweiten Quartal sollen Symbian-Entwickler eine SQL-Datenbank in ihren Anwendungen nutzen können, denn die von Nokia dominierte Entwicklerfirma Symbian Inc. integriert das freie SQLite (www.sqlite.org) in ihr Betriebssystem für Mobilgeräte. Die eingebettete Datenbank findet bisher unter anderem in Mozillas Firefox und diversen Apple-Programmen wie dem Adressbuch Verwendung. Sie ist in C geschrieben, für andere Programmiersprachen wie C++ und Java gibt es Wrapper. Außerdem stellen JDBC- und ODBC-Treiber Verbindung zu anderen Programmen her. SQLite bietet zwar Transaktionen, prüft Daten jedoch nur lax: Die meisten fehlerhaften Eingaben akzeptiert es klaglos und speichert sie als Strings. Constraits für Fremdschlüssel erzwingt SQLite nicht, es kennt auch keine GRANT- und REVOKE-Befehle.

Hewlett-Packard integriert Opsware

HP hat die im vergangenen Jahr übernommenen Opsware-Lösungen zur RZ-Automatisierung in die eigenen Managementwerkzeuge integriert. Workflows verknüpfen diese mit den Komponenten für die IT-Überwachung, -Analyse und -Steuerung des operativen IT-Betriebs. Mit den Tools lassen sich Service-Management-Prozesse wie das Ereignis- und Veränderungsmanagement über alle Domänen hinweg automatisieren. Eine Schlüsselrolle hierbei übernimmt die ehemalige Opsware-Komponente Operations Orchestration, die als zentrale Steuerungsinstanz der HP-Software für das Management des operativen IT-Betriebs dient. Die hinterlegten Abläufe verknüpfen Funktionen wie das Messen von Antwortzeiten, die Fehlerdiagnose, den Service Desk sowie das Konfigurieren von Netz- und Speicherkomponenten, Servern und Clients. Auf diese Weise sollen Erkenntnisse aus der IT-Überwachung, etwa schlechte Antwortzeiten, automatisch Aktionen wie Diagnose und Rekonfiguration auslösen.

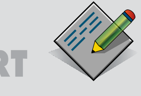
Ursachen kritischer Last grafisch aufbereitet

Das Netzmanagement-Werkzeug Scrutinizer Version 5.5 von Plixer, das hierzulande der Distributor PSP anbietet, analysiert den Netzwerkverkehr auf Basis von Netflow- und Sflow-Daten. Detailliert lässt sich durch die Analyse der Informationen des IP-Datenstroms sowie der Erfassung des Netzwerkverkehrs feststellen, welches Endsystem die kritische Last produziert, welche Applikation oder welches Protokoll in Aktion tritt und welche Netzwerkverbindungen betroffen sind. Vom Scrutinizer-Server gewonnene Informationen sind grafisch aufbereitet von jedem Browser aus abrufbar. Die zur Verfügung gestellten Netzwerkkarten lassen sich über das Web konfigurieren und per Drag and Drop variieren. Eine Visualisierung globaler Netze vereinfacht eine Schnittstelle zu Google Maps.

Accenture identifiziert mit Sun

Sun Microsystems und Accenture bringen gemeinsam die „Smart Identity Solution“ heraus. Sie unterstützt das sogenannte Identity Establishment (Identitätsbestätigung) sowie die sichere Authentifizierung, indem sie sowohl physische als auch digitale Systeme wie Smartcard oder Biometrie einbezieht. Unter dem Strich soll so ein gesicherter unternehmensweiter Identitätsmanagement-Prozess umsetzbar sein. Außer der Smart Identity Solution umfasst das „sichere“ Angebot von Accenture die Tools Enterprise Identity Management Solution, Solution for Control and Compliance (mit Einbindung von SAPs GRC – Governance, Risk and Compliance), SOA Jumpstart Solution for Sun Java und Secure SOA Solution. Die Sicherheitsprodukte basieren auf Suns Java System Identity Management Suite, der Java Composite Application Platform Suite (Java CAPS), Solaris sowie dem Java System Portal Server.

KURZ NOTIERT



Bündnis: iET Solutions ist eine Partnerschaft mit Criston eingegangen. Die Zusammenarbeit zwischen dem IT-Servicemanagement von iET und dem PC-Lifecycle- und Schwachstellen-Management von Criston soll die Verfügbarkeit der IT-Infrastruktur erhöhen und das Risikomanagement verbessern.

Automatisiert: BMC Software übernimmt Bladelogic, einen Anbieter von Automatisierungssoftware für Rechenzentren, für 800 Mio. Dollar. Bereits vor der Akquisition hatten beide Firmen zusammengearbeitet.

PyCon: Python 3 in Sicht

Mitte März zog die amerikanische Python-Konferenz (PyCon) in Chicago mehr als 1000 Besucher aus aller Welt an; mit acht Tagen war es die bislang längste. Etwa 30 Tutorien boten Stoff für Einsteiger und erfahrene Programmierer. 140 Vorträge zu Sprache, Bibliotheken, Frameworks, Scientific Computing sowie zahlreiche Erfahrungsberichte füllten die Konferenztage.

In seiner traditionellen Keynote bemerkte Python-Erfinder Guido van Rossum, dass er zum letzten Mal auf einer PyCon über Python 3 im Futur reden müsse, denn im Herbst soll die Dreierversion endlich erscheinen. Vorab-Releases sind schon erhältlich. Weitere Keynotes hielten unter anderem Van Lindberg, der die „Intellectual Property“ und „Open Source“ aus der Sicht eines Juristen beleuchtete, sowie Mark Hammond, der das Verhältnis zwischen Python und Mozilla darstellte.

Die Vielfalt der Python-Community spiegelte sich im Profil der Sponsoren wider: Google, Microsoft, Sun, O’Reilly – ein deutliches Zeichen für die wachsende Verbreitung und kommerzielle Nutzung der Sprache. Die gesamte Konferenz ist inzwischen auf Youtube zu sehen (www.youtube.com/user/pycon08). Im nächsten Jahr wird die PyCon wieder in Chicago stattfinden.

Christian Theune

KURZ NOTIERT



Enterprise-Suche: Mit der Version 8.5 ihrer Omnifind Enterprise Software bietet IBM durch Updates der Lotus-Produkte Quickr und Connection bessere Suchmöglichkeiten in sogenannter Social Software. Außerdem enthält die neue Version eine Analyse der besten Ergebnisse, deren Metadaten Grundlage einer grafischen Aufbereitung sind.

Browsertest: Sowohl die Entwickler von Webkit (das Apples Safari nutzt) als auch Opera konnten melden, dass die Produkte den schwierigen Browsertest Acid3 geschafft hätten (www.webstandards.org/action/acid3/).

PDF-Konvertierung Softvision Development aus Fulda bietet unter www.webpdf.net einen kostenlosen Dienst an, der aus über 100 Dateiformaten PDF erzeugt. Dokumente dürfen bis zu 4 MByte umfassen und unter anderem Text-, Tabellenkalkulations- und Präsentationsformate enthalten.

CMS in a box: Der taiwanesische NAS-Hersteller Qnap (www.qnap.com) bietet seine TS-409 Turbo NAS-Serie jetzt mitsamt dem CMS Joomla an, was MySQL und PHP einschließt.

Online-Enzyklopädie: Anders als vorgesehen hat die Verlagsgruppe B.I. & F.A. Brockhaus Mitte April ihr geplantes Wissensportal mit 300 000 Stichwörtern noch nicht eröffnet. Der Starttermin ist offen. Ob es eine 22. Auflage der Enzyklopädie geben soll, bleibt unklar, die Nachfrage nach der derzeitigen sei nach der Ankündigung des Portals gestiegen, heißt es beim Verlag.

ISO standardisiert Microsofts OOXML

Am 2. April haben die internationale Standardisierungsorganisation ISO und die internationale elektrotechnische Kommission (IEC) innerhalb ihres Joint Technical Committee 1 (JTC 1) Microsofts schon bei der Ecma als Standard 376 verabschiedetes Datenformat Office Open XML als ISO/IEC DIS 29500 anerkannt.

Erforderlich waren dafür zwei Drittel der Stimmen der im Komitee teilnehmenden Staaten und nicht mehr als ein Viertel Ablehnungen. Diese Bedingungen waren mit 75 % beziehungsweise 14 % erfüllt. Im Februar hatte ein Ballot Resolution Meeting (BRM, eine Art Abstimmungsnachbesprechung) stattgefunden, währenddessen das JTC die Kommentare einzelner Staaten diskutierte. Im September 2007 hatte OOXML noch keine ausreichende Mehrheit für die Standardisierung gefunden.

Im Umfeld der Entscheidung hat es offenkundig Irregularitäten gegeben. Steve Pepper, Vorsitzender des zuständigen Gremiums des norwegischen Normungsinstituts, hat formellen Protest dagegen eingelegt, dass Norwegens Ja berücksichtigt wird, weil 80 % der Gremiumsmitglieder für ein Nein waren.

Zu den ISO-Standards im Umfeld der Bürokommunikation gehören außer dem OOXML-Konkurrenten Open Document Format (ODF, ISO/IEC 26300) sowie zwei PDF-Varianten (Langzeitarchivierung, ISO 19005-1 und Druckvorstufe, ISO 15930). Für Mai hat Microsoft die endgültige Version seines OOXML-SDK angekündigt (siehe auch das Editorial, S. 3).

Apples Webbrowser Safari 3.1

Apples Webbrowser Safari liegt jetzt in der Version 3.1 vor – nur ein kleiner Sprung vom Vorgänger 3.0.4. Vor allem hinsichtlich Standards haben sich einige Änderungen ergeben. So unterstützt der Browser jetzt Webfonts nach den CSS 3, kennt die Elemente *audio* und *video* des noch in Entwicklung befindlichen HTML 5 (www.w3.org/html/wg/html5/) und erlaubt SVG-Grafiken im Element *img*. Leistung und Stabilität bezeichnet Apple als verbessert, und für die Windows-Variante gilt, dass sie signierte Java-Applets unterstützt und auf 16 Sprachen vorbereitet ist. Erhältlich ist die neue Version entweder über die Software-Aktualisierung auf Macintosh-Rechnern oder unter www.apple.com/safari/.

Web: Ältere brauchen länger

User-Interface-Guru Jakob Nielsen hat in seiner „Alertbox“ genannten Kolumne Ende März den Einfluss des Alters auf den Umgang mit dem Web diskutiert (www.useit.com/alertbox/middle-aged-users.html).

Nach seinen Untersuchungen werden die Mainstream-Surfer – die Altersgruppe zwischen 25 und 60 – bei der Benutzung von Websites jedes Jahr um 0,8 % langsamer. Das bedeutet im Laufe von 40 Jahren immerhin 32 %. Wegen der Beschleunigung des Alterungsprozesses geht Nielsen davon aus, dass Übersechzigjährige sogar um 74 % langsamer sind als die 40 Jahre Jüngeren.

Progress: Semantische Datenintegration

Der DataXtend Semantic Integrator (SI) von Progress soll die Datenintegrität in SOA-Umgebungen gewährleisten. Dazu fasst er die Punkt-zu-Punkt-Verbindungen zwischen verschiedenen Anwendungen an einer zentralen Stelle zusammen. SI bietet darüber hinaus ein Design-Werkzeug sowie eine Laufzeitumgebung. Über den Designer lassen sich Schemata für Datenquellen und -dienste sowie sogenannte Common Data Models (CDM) importieren – etwa für die Telekommunikationsbranche. Je nach Semantik und Syntax des Schemas wandelt er die angeforderten Daten in die allgemein „verständliche“ Sprache um und bildet sie auf die nächste entsprechende Applikation ab.

Impact-Analysen, die Modifikationen an den Daten und deren Auswirkungen auf die Quellen erkennen, kann der Benutzer mit dem Designer ebenfalls durchführen. In der aktuellen Version 8.3 hat Progress die Funktion „Change Data Capture“ in die Laufzeitumgebung integriert. Sie steuert den Informationsfluss zwischen den verschiedenen Datenbanken, die ein gemeinsames Datenmodell verwenden, und aktualisiert automatisch das CDM. Zurzeit unterstützt SI lediglich Oracle-Datenbanken als Data Distribution Sources. Zusammen mit einem Enterprise Service Bus lässt sich die Laufzeitumgebung als Dienst oder Applikationsserver auch außerhalb einer SOA einsetzen. *Susanne Franke*

BPM-Suite für die Fachanwender

Mithilfe der BPM-Suite (Business Process Management) M3O von Vitria sollen die Fachabteilungen Geschäftsprozesse eigenständig modellieren und gemeinsam mit der IT-Abteilung verwalten. Die Software bietet eine auf BPMN (Business Process Modeling Notation) beruhende Umgebung, in der die Anwender Geschäftsabläufe in einzelnen Schritten aufbauen können. Aufgabe der IT bleibt weiterhin die technische Anbindung der involvierten Anwendungen und Systeme. Fach- und IT-Abteilung greifen rollenbasiert auf dieselbe Umgebung sowie das Repository zu, in dem die Prozesse liegen. Vitria liefert die BPM-Suite mit einem JBoss-Server aus. Sie basiert auf dem ehemaligen Business Accelerator, der nun unter dem Namen M3O ESB firmiert. Ebenfalls Bestandteil des Pakets ist der Exception Manager, der regelgesteuert Ausnahmesituationen und Fehler in den Prozessen erkennt und behandelt. *Susanne Franke*

KURZ NOTIERT

Kommerzanalyse: Webtrends, Anbieter für Webanalyse-Software, und Intershop arbeiten zusammen. Im Rahmen der Kooperation hat Intershop das Shop-Analyse-Werkzeug Webtrends Analytics 8 in seine E-Commerce-Software Enfinity Suite 6 eingebaut.

Zusammenführung: Projectplace und Netviewer haben ihre Partnerschaft erneuert. Danach lässt sich Netviewer five mit VoIP- und Videofunktion in das On-Demand-Angebot zum Projektmanagement von Projectplace einbinden.

Besser untersucht: Die neue Release der Enterprise Intelligence Platform SAS9.2 von SAS bietet erweiterte Analysefunktionen. Diese sollen helfen, komplexe Simulationen und Vorhersagen inklusive Was-wäre-wenn-Szenarien durchzuführen. Verbessert hat man angeblich auch den Aufbau der Optimierungsmodelle.

SaaS-CRM: Parallels erweitert seine Automatisierungslösung für Rechenzentren um den Support für Microsofts Dynamics CRM 4.0. Service Provider können dieses Angebot für das Management von Kundenbeziehungen somit in ihr On-Demand-Angebot aufnehmen.

Semiramis findet neuen Grund

Gut ein Jahr nach der Übernahme von Teilen der insolventen Semiramis darf sich SoftM über die ersten Früchte seines Engagements rund um die in Java geschriebene Standardsoftware freuen. Mit 40 Abschlüssen im Jahr 2007 erreicht man die eigene Zielvorgabe allerdings nicht ganz. Die Umsatzzuwächse in den letzten Quartalen sowie die gut gefüllte Interessentenliste nähren jedoch große Hoffnungen auf lukrative Geschäfte in der Zukunft. Hilfreich ist, dass es seit diesem Monat endlich die Release 4.4 von Semiramis gibt.

Zu den Neuerungen zählen unter anderem Frameworks für Rechnungswesen, BI Cockpit und Business Process Management. Das Rechnungswesen basiert auf der Sharknex-Software, die SoftM mit der J2EE-Entwicklungsplattform Bison Solution der gleichnamigen Schweizer Firma umsetzte. Im Analyse/BI-Bereich verlässt sich SoftM auf Microsoft-Technik, die BI-Komponente benötigt daher einen SQL Server als Grundlage. Damit sich komplexe Transaktionen prozessorientiert steuern lassen, zog das Münchner Unternehmen zwischen Anwendungs- und Präsentationsschicht einen separaten Prozess-Layer ein. Er enthält die Ablaufbeschreibungen, die die Prozess-Engine zur Laufzeit ausführt. Die BPM-Software ist keine Eigenentwicklung, sondern basiert auf Xpert.ivy der Schweizer Soreco AG.

Ebenfalls neu ist eine Komponente für das Qualitätsmanagement, die Funktionen zum Generieren und Umsetzen von Prüfplänen für den Wareneingang bereitstellt. Zudem unterstützt Semiramis nun die Außenhandels- und Zollabwicklung gemäß der elektronischen Ausfuhranmeldung im Atlas-System der deutschen Zollverwaltung. In Kürze will SoftM den Partner für die On-Demand-Variante von Semiramis präsentieren. Dem Vernehmen nach soll sich das gehostete Angebot eher am ASP-Modell (Single Tenant) als an einem echten SaaS-Betrieb (Multi Tenant) orientieren.

SAP plant Business Intelligence neu

Nach SAPs Übernahme von Business Objects nimmt die Portfoliozusammensetzung im Bereich Business Intelligence peu à peu Gestalt an. Für bestehende Produkte will man zwar für mindestens fünf Jahre den Support gewährleisten, gleichzeitig ist aber bei den BI-Werkzeugen das große Aufräumen angesagt. Einer Analyse des Würzburger Business Application Research Center (BARC) zufolge werden beispielsweise SAP-Eigengewächse wie BI Integrated Planing bestenfalls als technische Komponenten überleben. Denn für Planungsaufgaben gilt die Software der im vergangenen Jahr erworbenen Outlooksoft, die nun unter der Bezeichnung SAP BPC (Business Planning and Consolidation) vermarktet wird, als künftiger Standard.

Pilot Software, eine weitere Akquisition, stellt die Basis für das strategische Management. Im Segment der Finanzkonsolidierung kommen die Produkte der Business-Objects-Tochter Cartesis zum Zuge. Perspektivisch möchte SAP die Tools zur Finanzkonsolidierung, das eigene SEM BCS, Outlooksofts Integrated Consolidiation sowie Cartesis zusammenführen. Dabei soll Cartesis die technische Grundlage bilden und die Frontends von Outlooksoft den Zugang ermöglichen. Andere Planungswerkzeuge wie die von Business Objects eingebrachten Produkte Planning XIR2/SRC und Extended Planning/Inea, die ihrerseits ebenfalls aus Übernahmen stammen, wird SAP nach Einschätzung von BARC nicht mehr aktiv weiterentwickeln. SAP BPC, deren Oberflächen auf Excel beziehungsweise Microsoft Office basieren, nutzt im Serverbereich ausschließlich Datenbanktechnik von Microsoft und Oracle. Es liegt auf der Hand, dass SAP mit Hochdruck daran arbeitet, zumindest ergänzend die Einbindung in die eigene Business-Warehouse-Technik voranzutreiben.

Topix führt Funktionen zusammen

Anfang des Jahres hat die Topix AG den Quellcode der auf der Datenbank 4D basierenden ERP-Software P4 Enterprise sowie die zugehörige Kundenliste vom Insolvenzverwalter der Parkstreet GmbH übernommen. Der neue Eigner beabsichtigt, den Support für P4 Enterprise so lange fortzuführen, bis der Umstieg auf das eigene, ebenfalls auf 4D basierende Topix 5 vollzogen ist. Mittelfristig will man vor allem Funktionen aus Lagerwirtschaft und Produktion aus P4 in Topix 5 überführen. Auch die Module Webshop und Publishing für datenbankgestützte Webseitengenerierung und Print-Katalogproduktionen sollen bei Topix überleben.

PLM in SAP einbinden

ECS bringt eine neue Version seines PLM Integrators (Product Lifecycle Management) auf den Markt. Mit dem als SAP-Partnerlösung zertifizierten XI-Adapter lassen sich Programme für das Product-Lifecycle-Management in die Exchange Infrastructure (XI) von SAPs Netweaver einbinden und in systemübergreifende Geschäftsprozesse integrieren. Das Abbilden der PLM- auf SAP-Objekte und umgekehrt erfolgt bis auf Attributebene über grafische Editoren. Neben einfachen 1:1-Zuordnungen kann der Entwickler komplexe Transformationen, Regelwerke und Mapping-Tabellen hinterlegen, um beispielsweise strukturierte Produktinformationen wie Stücklisten ineinander überführen zu können.

Projektmanagement in zwei Varianten

Onepoint Software, ein österreichischer Anbieter für Projekt- und Portfoliomanagementsoftware (PPM), hat die Version 8 seines Projektführungswerkzeugs Project vorgestellt. Zu den Neuerungen gehören beispielsweise anpassbare Projekt- und Ressourcentypen, konfigurierbare E-Mail-Nachrichten sowie ein erweitertes Dokumentenmanagement. Optional sind Module für Skills Management und Status-Reporting erhältlich. Sie lassen sich zusammen mit dem Hauptprodukt lizenzieren. Onepoint Project gibt es in einer kommerziellen und in einer Open-Source-Ausprägung. Letztere lässt sich von sourceforge.net/projects/opproject/ herunterladen.

Lawson peilt neue Kunden an

Den Lawson Process Flow Integrator gibt es nun auch als Zusatzprodukt zum Lawson M3 Enterprise Management. Die Webservice-fähige Software, seit Längerem schon bei Kunden im Gesundheitswesen, im öffentlichen Sektor und anderen Dienstleistern im Einsatz, hilft Unternehmen dabei, Geschäftsprozesse zu erstellen sowie festzulegen, wie der Datenfluss zwischen unterschiedlichen Geschäftsanwendungen (auch von Drittanbietern) aussehen soll. Dieses Produkt können nun auch Interessenten aus Fertigung und Handel ordern.

Major Release von PlanningIT

PlanningIT, das Planungswerkzeug der Berliner Alfabet AG soll das Zusammenwirken von Geschäft und IT verbessern. Die neue Release 4.0 bietet einige Erweiterungen, beispielsweise hat das Softwarehaus dem Produkt eine neue Plattform für die Workflow-Automatisierung spendiert, mit der sich Prozesse aufbauen, formalisieren und überwachen lassen. Über das Milestone Tracking will man die IT-Governance besser abdecken. Und Blueprint Planning und Migration Planning erhöhen die Konsistenz, Vollständigkeit und Effizienz bei der Planung von IT-Landschaften. PlanningIT 4.0 ist auf Subskriptionsbasis (SaaS) oder in einer unbefristeten Lizenz erhältlich.

KURZ NOTIERT

Zugelegt: Die Stepstone ASA verdoppelte im abgelaufenen Geschäftsjahr den Umsatz auf 98,5 Mio. €. Das EBITDA wuchs im gleichen Zeitraum von 9,8 Mio. auf 22,4 Mio. €. Die Einnahmen im Portalgeschäft legten dabei um 67 % auf 58,3 Mio. € zu.

Vage: Auch im laufenden Jahr soll der PC-Absatz nach Gartner zweistellig auf weltweit rund 293 Mio. Einheiten zulegen. Allerdings können die rezessiven Tendenzen der US-Wirtschaft, ein verlangsamtes Wirtschaftswachstum in China sowie ein hoher Ölpreis das Wachstum noch unter zehn Prozent drücken.

Ein Drittel mehr: Der IT-Dienstleister Hexaware Technologies Ltd. steigerte 2007 den Umsatz um 35,1 % auf 252,94 Mio. $. Der Nettogewinn lag bei 26,78 Mio. $.

Geschluckt: SAS übernahm Teragram, einen US-Anbieter von Textanalyse-Software. Mit der Akquisition will der Business-Intelligence-Spezialist seine Text-Mining- und Analyse-Angebote um Funktionen für Enterprise Search über PCs und mobile Endgeräte ausdehnen.

Getrotzt: Ungeachtet der US-amerikanischen Konjunkturschwäche verdoppelte Blackberry-Anbieter Research in Motion (RIM) im Geschäftsjahr 2007/2008 den Umsatz auf fast 6 Mrd. $. Den Gewinn baute die kanadische Firma auf 1,3 Mrd. $ aus. Ingesamt zählt RIM jetzt 14 Millionen Blackberry-Abonnenten.

Geplatzt: Nicht einverstanden aufgrund von Sicherheitsbedenken waren die US-Behörden mit dem Kauf von 3Com durch die Investorengesellschaft Bain und den chinesischen Netzequipment-Hersteller Huawei.

Wechsel in der SAP-Führungsetage

Ernte einfahren

Achim Born

Mit der erwarteten Neuordnung an der Unternehmensspitze stellt SAP die Weichen für die Zukunft. Auch wenn es zunächst keine großartigen Veränderungen in der Unternehmensstrategie geben soll, zeigen die jüngsten Ankündigungen eins: SAP will mehr Geld verdienen.

Nun ist der Wechsel an der SAP-Spitze offiziell. Den bisher stellvertretenden Vorstandssprecher Léo Apotheker hat der Aufsichtsrat am 2. April zum gleichberechtigten zweiten Vorstandssprecher neben Henning Kagermann ernannt. Ab Mai kommenden Jahres, wenn der Vorstandsvertrag des aktuellen SAP-Chefs Kagermann ausläuft, leitet der Wahl-Pariser die Geschicke des größten deutschen Softwarehauses als alleinige Spitze.

An der Bestellung von Apotheker überrascht allenfalls der Zeitpunkt. Dass der Vertriebsprofi zum neuen Chef erkoren wird, galt spätestens nach dem Abgang des damaligen Technologievorstandes Shai Agassi als ausgemacht. Nachdem der als Ziehsohn des SAP-Mitgründers und Aufsichtsratsvorsitzenden Hasso Plattner gehandelte Agassi an seiner Ungeduld scheiterte und im vergangenen Jahr überraschend das Handtuch warf, war das Nachfolgerennen im Grunde entschieden. Mit der gleichzeitigen Berufung des einstigen Amerika-Verantwortlichen Bill McDermott zum weltweiten Vertriebschef sowie von Jim Hagemann Snabe zum Verantwortlichen für die Entwicklung der SAP Business Suite und die Netweaver-Plattform und von Erwin Gunst zum Chief Operating Officer (COO) sind die Weichen für die Zukunft im SAP-Vorstand gestellt. Auch Forschungsvorstand Peter Zencke wird seinen zum Jahresende auslaufenden Vertrag nicht verlängern. Als Berater soll die treibende Kraft hinter der neuen Business-ByDesign-Software jedoch dem Unternehmen verbunden bleiben.

Der SAP-Vorstand ist in der neuen Zusammensetzung fraglos verkaufs- und controllinglastig. Im Unterschied zu den bisherigen Vorsitzenden besetzt mit Apotheker, der fünf Sprachen beherrscht, erstmals ein Nichttechniker den Chefsessel. Es wird deshalb allgemein mit einer stärkeren Marketing- und Verkaufsorientierung des Softwarekonzerns aus Walldorf gerechnet.

Die jüngste Vergangenheit war von Entwicklungsaktivitäten – im SAP-Jargon Innovationen – geprägt, darunter dem Einzug der serviceorientierten Softwarearchitektur in die eigene Anwendungslandschaft und der neuen, von Grund auf prozess- und serviceorientiert-entworfenen Lösung für den Mittelstand (Business ByDesign) samt einem neuen SaaS/On-Demand-Geschäftsmodell.

Jetzt soll die Ernte eingefahren werden. Da ist ein harter Controller mit Blick auf die Quartalszahlen für die Aktionäre wichtig. Auch wenn es in nächster Zeit keine radikalen Änderungen in der Unternehmensstrategie geben soll, deuten erste Äußerungen von Apotheker einen leichten Richtungswechsel an. Sein Credo lautet, dass sich Investitionen rechnen beziehungsweise beim Kunden ankommen (vulgo: absetzbar sein) müssen. Zudem kündigte er in einen FAZ-Interview an, die Entwicklungskosten für neue Software, die zuletzt 14 % vom Umsatz erreicht hatten, künftig wieder auf frühere Größenordnungen stutzen zu wollen.

Dass es bei SAP künftig verstärkt ums Verdienen geht, zeigte die unlängst verkündete Neuordnung der Wartungskonditionen für Neukunden. Erhielt man bislang mit jährlichen Gebühren von 17 % des Lizenzpreises einen Basissupport, steht seit Februar allein noch der zuvor als Premium beworbene Enterprise-Support für jährlich 22 % zur Wahl. Selbst wenn SAP in puncto Wartungskosten nur mit dem Erzkonkurrenten Oracle gleichzieht, dürften SAP-Anwender über diesen Schritt kaum glücklich sein.

Aber auch für die Mitarbeiter zeichnet sich ein raueres Klima ab. Denn im Vergleich zum ruhigen, kühlen Kagermann zeichnen den Chef in spe mehr Temperament und Härte in der Sache aus. Es ist deshalb damit zu rechnen, dass etwa Entwickler bei verpassten Ziel- und Zeitvorgaben auf weitaus weniger Verständnis als bislang hoffen dürfen.

All diese Maßnahmen dienen letztlich dem Ziel, spätestens Ende 2010 eine Umsatzrendite von 35 % zu erreichen. (WM)





Die Doppelspitze soll's bringen: Henning Kagermann (links) und Léo Apotheker (rechts) wollen SAP ein Jahr zusammen führen.

Weltweiter Server-Markt: Mehr Verkäufe

Im vergangenen Jahr konnten die Hersteller weltweit mit 8,8 Millionen Servern rund 7,4 % mehr Systeme an den Kunden bringen. Allerdings legten die Umsätze nicht im Gleichschritt zu; sie wuchsen nur um 3,8 % auf circa 54,8 Mrd. $. Innerhalb der einzelnen Serverklassen hat Gartner Dataquest allerdings unterschiedliche Entwicklungen registriert. So gibt es bei den RISC/Itanium-basierenden Unix-Servern eindeutig die Tendenz zu kostspieligen Systemen, da die Auslieferungen um 13,8 % zurückgingen, obgleich die Einnahmen um 1,7 % zulegten. Um 44,5 % steigerten sich die Umsätze mit Blade-Servern, auch wenn man nur knapp 20 % mehr Systeme ausliefern konnte. Dabei dominieren HP mit 41,7 % und IBM mit 30,9 % Anteil an den Verkäufen eindeutig diese Server-Segment.

Mit Blick auf den Gesamtmarkt ist IBM mit 17 Mrd. $ weiterhin die Nummer eins in der Rangliste der umsatzstärksten Hersteller, es folgt HP mit 15,5 Mrd. $. Dell verdrängte im vergangenen Jahr Sun vom dritten Platz. Die umsatzstärksten Anbieter konnten im Vergleich zum Vorjahr nahezu alle zulegen. Allein FSC wies einen Einnahmenrückgang auf. Zieht man dagegen die Auslieferungen heran, sind Sun und IBM die Wachstumsverlierer. Ansonsten gibt es im Vergleich zum Vorjahr keine Veränderung in puncto Rangfolge. Es führt weiterhin HP vor Dell, während IBM nur als drittgrößter Lieferant gelistet wird.

Weltweiter Server-Markt 2007

nach Umsätzen

Unternehmen	Umsatz 2007	Marktanteil	Umsatz 2006	Marktanteil	Wachstum
IBM	17,0	31,1	16,9	32,0	0,8
HP	15,5	28,3	14,2	27,0	8,8
Dell	6,2	11,4	5,5	10,5	13,2
Sun	5,9	10,8	5,7	10,8	3,5
FSC	2,4	4,5	2,5	4,8	-1,5
andere	7,6	13,9	7,8	14,9	-3,7
gesamt	54,8	100	52,8	100	3,8

Umsatzzahlen in Milliarden Dollar, alle anderen Angaben in Prozent

nach Auslieferungen

Unternehmen	Auslieferungen 2007	Marktanteil	Auslieferungen 2006	Marktanteil	Wachstum
HP	2636	29,8	2261	27,7	16,6
Dell	1894	21,4	1783	21,7	6,2
IBM	1282	14,5	1293	15,7	-0,9
Sun	338	3,8	368	4,5	-8,3
FSC	292	3,3	256	3,1	13,9
andere	2396	27,1	2270	27,6	5,6
gesamt	8841	100	8233	100	7,4

Stückzahlen in Tausend, alle anderen Angaben in Prozent

Itelligence: Besser als erwartet

Die Bielefelder Itelligence AG, Dienstleister im SAP-Umfeld, freut sich über ein Umsatzwachstum von 16,5 % auf 190,9 Mio. €. Mit dem Jahresabschluss wurden die Erwartungen deutlich übertroffen, die zuvor bei 175 bis 185 Mio. € lagen. Das operative Ergebnis erreichte einen Wert von 11,5 Mio. € (+62,0 %). Die größte Umsatzsteigerung erzielte der Bereich Beratung, mit einem Plus von +18,3 % auf 113,1 Mio. €. In Folge bleibt das Segment mit nunmehr 59,2 % stärkster Unternehmensbereich. Mit Lizenzen wurden 23,8 Mio. € (+15,5 %) Umsatz erzielt. Das Segment Outsourcing & Services steuerte 53,6 Mio. € (+14,3 %) zu den Einahmen bei. Wie in den vergangenen Jahren bildeten Deutschland und Österreich die umsatzstärkste Region. In diesen Ländern wurde ein Anteil von 96,3 Mio. € (+34,7 %) des Gesamtumsatzes erwirtschaftet. Amerika steuerte 23,9 %, Westeuropa 16,6 % (Vorjahr: 17,3 %) und Osteuropa 7,4 % bei.

Red Hat bleibt offen für Geschäfte

Red Hat bewies wieder, dass sich mit Open Source durchaus gute Geschäfte machen lassen. Den Umsatz im Geschäftsjahr 2008 (Abschluss 29. Februar) konnte der Linux-Distributor um 31 % auf 523 Mio. $ ausbauen. Der Subskriptionsumsatz kletterte um 32 % auf 449,8 Mio. $. Der Nettogewinn nach US-GAAP lag mit 76,8 Mio. $ rund 28 % höher als im Vorjahr. Ohne Berücksichtigung von Einmalbelastungen und Sonderfaktoren betrug der Gewinn 152,9 Mio. $, nach 115,9 Mio. $ im Jahr 2007. Dass auch künftig die Geschäfte mit Unternehmenskunden gut laufen, zeigt die Entwicklung des „deferred revenue“. Diese im deutschen Rechnungswesen als passiver Rechnungsabgrenzungsposten bezeichnete Bilanzgröße legte um 40 % auf rund 472 Mio. $ zu. Der RAP nennt den Wert bereits erhaltender Zahlungen für Leistungen, die wie bei mehrjährigen Subskriptionsverträgen noch in den kommenden Bilanzperioden anfallen und deren Umsätze erst zu diesem Zeitpunkt verbucht werden.

GFT Technologies weiterhin erfolgreich

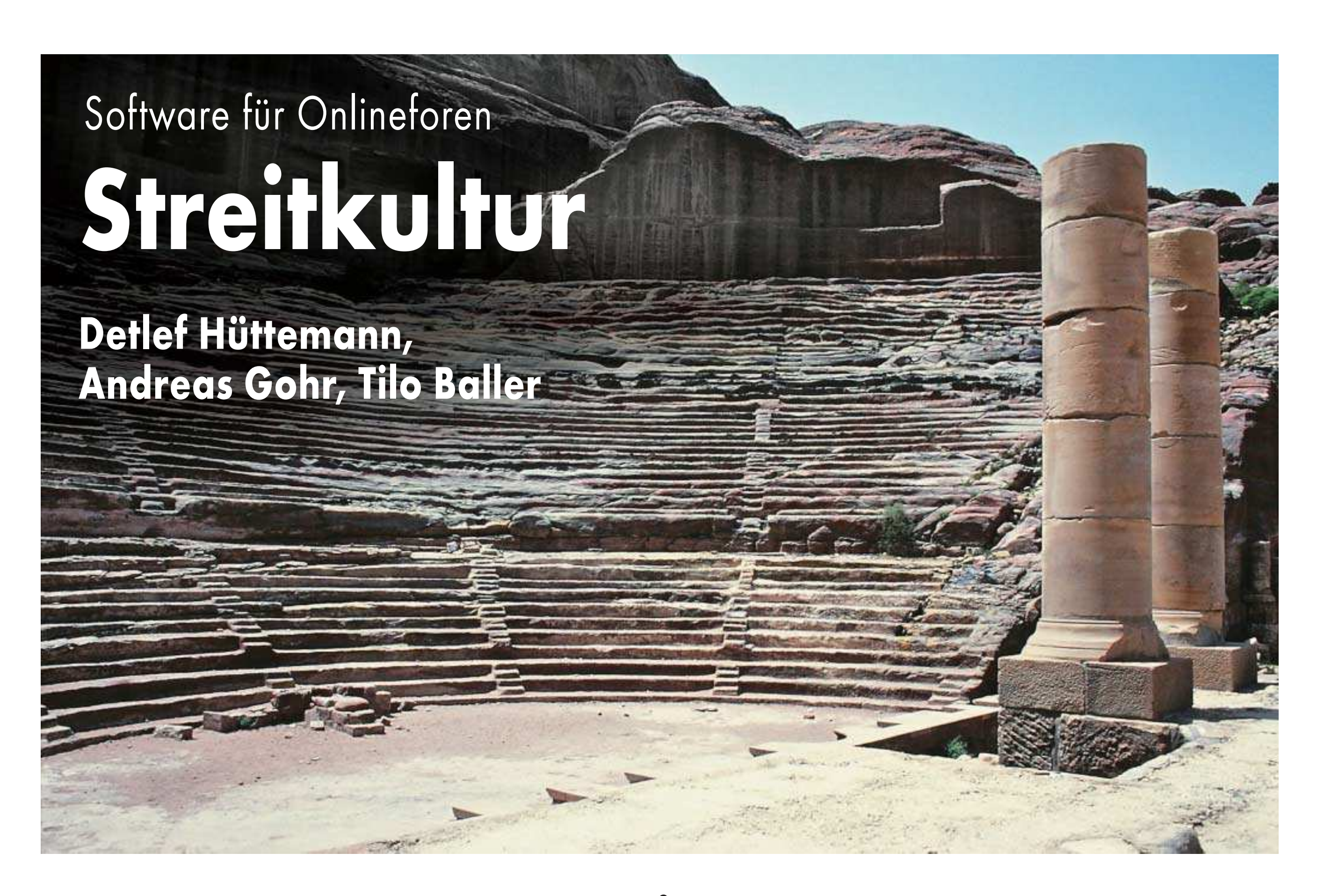
Mit 247,1 Mio. € lag der Gesamtumsatz der GFT Technologies AG 42 % über dem Vorjahreswert. Entsprechend stieg das Ergebnis vor Steuern um 85 % auf 12,4 Mio. €. Mit 140,4 Mio. € war Resourcing der umsatzstärkste Geschäftsbereich; sein Anteil am Gesamtumsatz beträgt nun rund 57 %. Dieser Geschäftsbereich wurde im vergangenen Jahr auf die Standorte London und Zürich ausgeweitet. Der anhaltende Fachkräftemangel sowie die Tendenz, IT-Projekte flexibel mit freiberuflichen IT-Spezialisten zu besetzen, lässt das GFT-Management hier auf weiterhin gute Geschäfte hoffen. Auch mit Services erzielte die GFT-Gruppe 2007 ein ordentliches Wachstum. Die Einnahmen legten um 22 % auf 100,8 Mio. € zu. Die Unternehmenssparte Software schloss dagegen bei einem Umsatz von 5,9 Mio. € unter den Erwartungen ab.

Mehr Umsatz, mehr IT

Unternehmen, die eine im Branchendurchschnitt höhere Rendite erzielen, investieren 3,4 % mehr in IT. Renditeschwache Unternehmen hingegen beschneiden sogar ihre IT-Budgets im Vergleich zum Vorjahr. Zu diesem Ergebnis kommt die IT-Studie 2008, die das Handelsblatt und die Unternehmerberatung Droege & Comp. im März vorstellten. Laut den Antworten der 359 befragten Firmen mit Sitz in Deutschland, Österreich und der Schweiz werden vermehrt Aufgaben an externe Helfer abgegeben. Wie in den Vorjahren steht die IT-Infrastruktur oben auf der Agenda der Investitionsprojekte in den Unternehmen. Bei den Ausgaben für Anwendungen hat sich dagegen eine leichte Verschiebung ergeben. Hatte im Vorjahr die Stärkung des Vertriebs die Budgets geprägt, steht in diesem Jahr die Produktion mit einem Budgetanteil von 22 % im Mittelpunkt der Investitionen. Ansonsten ist im RZ das große Aufräumen angesagt.

Wettbewerb: „Deutscher Internetpreis“

Mitte März gab der Bitkom den Startschuss zum diesjährigen Wettbewerb „Deutscher Internetpreis“, der unter dem Slogan „Mittelstand interaktiv“ steht. Kleine und mittlere Unternehmen, die innovative Internet-Anwendungen erfolgreich nutzen, können ihre Teilnahme bis 1. August 2008 online anmelden. Die Wettbewerbsbeiträge müssen sich dabei auf die Anwendungsbereiche interaktive Kommunikation, digitale Geschäftsprozesse sowie mobile Businessmodelle im Mittelstand beziehen. Die drei siegreichen ITK-Anwendungen werden mit 25 000, 20 000 und 15 000 Euro prämiert. Die Teilnahmebedingungen finden Interessierte unter www.deutscher-internetpreis.de.



Software für Onlineforen

Streitkultur

Detlef Hüttemann,
Andreas Gohr, Tilo Baller

Die Lust, im Internet spontan seine Meinung zu äußern, hat Onlineforen einen anhaltenden Schub versetzt. Dementsprechend vielfältig sind die Softwaresysteme zur Einrichtung der Foren. Eine Marktübersicht mit exemplarischen Ausflügen.

Was einst im akademischen Umfeld mit Netnews und Mailinglisten begann, hat sich heute im privaten und kommerziellen Bereich breit durchgesetzt. Onlineforen sind in Unternehmen für den Kundensupport einsetzbar; zur Diskussion auf Medien-Sites und zur Selbstdarstellung beispielsweise von Schulen und Vereinen dienen sie als Basis, um Diskussionen zu strukturieren.

Nach einem Überblick über typische und sinnvolle Features moderner Forensysteme stellt dieser Artikel die folgenden acht Applikationen detaillierter vor: punBB, phpBB, Vanilla, Unclassified Newsboard, vBulletin, Burningboard, JForum und YetAnotherForum.Net. Viele weitere etablierte Applikationen sind auf dem Markt verfügbar – eine Onlineübersicht bietet beispielsweise Forummatrix [a].

Onlineplattformen für Foren beziehungsweise Bulletinboards gibt es viele, das Nutzungsprinzip ist jedoch bei allen Systemen weitestgehend gleich: Eine Person eröffnet eine Diskussion (Thread), indem sie einen Beitrag (Posting) schreibt. Andere Personen lesen diesen und schreiben ein Antwort-Posting – oder eine Antwort auf eine Antwort, womit die Diskussion bereits im Gange ist.

Moderation der Foren

Das wichtigste Unterscheidungskriterium der Systeme ist die Art, wie die Beiträge angeordnet sind: entweder hierarchisch als Baum oder chronologisch sortiert. Hierarchische Ansichten stellen zwar den Bezug zum jeweiligen Vorredner klar, können aber zu entkoppelten Teildiskussionen führen. Bei einer chronologischen Anordnung dagegen fehlt die direkt logische Verknüpfung zwischen zwei Beiträgen. Sobald auf ein älteres Posting geantwortet wird, muss der Diskussionsteilnehmer den Bezug zum Vorredner über Zitate herstellen; Zitatfunktionen der Software erleichtern dies.

In der Regel erwartet ein Anwender, dass er seine Diskussionsbeiträge ungefiltert und unverzüglich veröffentlichen kann. Es ist naheliegend, dass dies Spammer anzieht wie Motten das Licht – die Forensysteme kontern mit Abwehrmechanismen. Gegen einzelne Spammer oder notorische Nörgler helfen kurzfristig IP-Bannlisten. Automatisierten Spambots wird mit Flood Control (Kontrolle der Anzahl der Beiträge in einem Zeitraum) und Captchas mehr oder minder erfolgreich Widerstand geleistet. Gelangt dennoch ein offensichtlich fragwürdiger Beitrag an die Öffentlichkeit, bleiben Moderationswerkzeuge als Ultima Ratio, um den unerwünschten Content zu entfernen.

Grundsätzlich kann der Betreiber Beiträge nachträglich editieren oder ganze Diskussionsstränge löschen. Auch wenn einem der Eingriff in die freie Meinungsäußerung missfällt – wer ein Diskussionsforum betreibt, kann für von Benutzern eingestellte beleidigende oder strafbare Inhalte haftbar gemacht werden. Sofern er als Betreiber über die Inhalte in Kenntnis gesetzt wurde, ist er

zur Löschung des Beitrages verpflichtet [b]. Der unmittelbar folgende Artikel „Forensisch“ reflektiert den aktuellen Stand der Rechtsprechung.

Bei einem anderen Verfahren geht es um die Anordnung der Threads: Markiert ein Moderator einen Thread als sticky, steht er in den Übersichtsseiten ganz oben – normalerweise listen die Systeme aktuelle Threads zuerst. Sticky Threads enthalten häufig grundsätzliche Informationen wie Netiquette, Nutzungsbedingungen oder FAQs. Sticky-Threads lassen sich – wie alle anderen Threads auch – schließen, wobei eingestellte Inhalte sichtbar bleiben, Benutzer können sie aber nicht mehr weiter diskutieren.

Customizing und Security

Mit einem weiteren Moderationswerkzeug lassen sich einzelne Threads aufteilen (Split Thread): Schweift eine Diskussion stark vom Thema ab, kann ein Moderator einzelne Beiträge in einen komplett neuen Thread abspalten; das hilft Übersichtlichkeit zu erhalten und Neuankömmlingen den Einstieg zu erleichtern. Um von vornherein eine inhaltliche Struktur zu bekommen, kann man Kategorien festlegen, unterhalb derer sich die eigentlichen Threads einordnen.

In der Regel ist es der Wunsch des Betreibers, ein prominentes und viel besuchtes Forum zu erhalten. Suchmaschinenfreundliche URLs, die den Betreff des Thread enthalten, können für ein besseres Ranking sorgen. Während die „Benutzersicht“ normalerweise lange Diskussionen auf mehrere blätterbare Seiten verteilt, bilden LoFi-Views komplette Themenstränge in reduzierter Form auf Einzelseiten ab. Sie enthalten damit hohe Verdichtungen von Inhalten und Schlagwörtern, ohne Suchmaschinen-Bots, beispielsweise durch Navigationselemente, zu verwirren. Zudem werden diese Views häufig als statische HTML-Seiten abgelegt, um den Server zu entlasten.

Um ein Forum gestalterisch dem Thema anzugleichen, lassen sich mit einem Skin-Editor im begrenzten Umfang Farben und Fonts anpassen – wer mehr will, muss selber Hand anlegen. Hilfreich für die Gestaltung ist es, wenn der benötigte (HTML)-Code getrennt von den Implementationsfunktionen vorliegt (Template-Konzept). Einige Forensysteme bieten Unterforen an, die durch individuelle Templates gestalterisch anzupassen sind. Zu groß darf allerdings die Erwartungshaltung an das Design nicht sein, der Grundaufbau ist bei fast allen Foren gleich: Breadcrumbe-Navigation, Forumliste, Thread-Liste und Statistiken bestimmen das Bild.

Soll neben der Layout-Anpassung eine Integration in einen bestehenden Web-Auftritt erfolgen, wird’s richtig schwierig. Zwar bieten die meisten Systeme Content Syndication via RSS an, sodass zumindest die Inhalte eines Forums in anderen Websites annonciert werden können. Eine Möglichkeit, aktiv zu diskutieren, ergibt sich hierdurch aber nicht. Forensysteme besitzen in der Regel eigene Implementierungen für die Verwaltung der Postings und Threads sowie für die Nutzer und ACLs. Offene APIs sind selten. Zumindest für Single-Sign-On (SSO) oder die Delegation der Authentifizierung an andere Unternehmensanwendungen findet man sporadisch Unterstützung.

Foren lassen sich mit individuellen Zugriffsrechten für das Lesen und Schreiben von Beiträgen für einzelne Nutzer ausstatten. Wer dieses exzessiv betreibt, freut sich über Benutzergruppen. Hier werden die Lese- und Schreibrechte initial für frei definierbare Gruppen vergeben. Die administrative Arbeit bei der Verwaltung der Benutzer beschränkt sich dann darauf, diese den passenden Gruppen zuzuordnen.

Foren sind wie alle Webapplikationen einem erhöhten Angriffsrisiko ausgesetzt. Wenn eine anonyme Anmeldung ausreicht, kann ein Angriff potenziell sogar „von innen heraus“ erfolgen, also von angemeldeten Usern der Community. In der Vergangenheit zeigten sich die Systeme besonders anfällig gegenüber Cross-Site Scripting und Remote Code Injections – Angriffsmethoden, bei denen unzureichend geprüfte User-Eingaben schadhaften Code in das System schleusen.

Eine besonders beliebte Angriffstechnik stellt das „Cross-Site Request Forgery“ (CSRF) dar: Hierbei nutzt der Angreifer die in allen Foren vorhandene Funktion, einen Link in einem Beitrag zu schreiben. Dieser Link ist nun so konstruiert, dass er auf eine Administrationsfunktion des Forums selbst zeigt – beispielsweise auf die Funktion zum Hinzufügen eines Nutzers zur Administratorgruppe. Der Link lässt sich mittels BBCode tarnen und in einem Neugier weckenden Zusammenhang posten. Sobald ein angemeldeter Administrator auf den präparierten Link klickt, wird die gewünschte Aktion ausgeführt. Glücklicherweise sind die meisten Forensysteme inzwischen vor solchen Angriffen geschützt.

iX-TRACT

- Forensoftware hat als Kommunikationsbasis die klassischen Usenet/Newsgroups fast vollständig verdrängt.
- Es gibt ein großes Angebot an kostenloser oder preiswerter Forensoftware.
- Die äußere Erscheinungsform ist weitgehend ähnlich, nur wenige Produkte entziehen sich der Konformität.
- Als Programmierparadigma werden Skiptsprachen wie PHP und objektorientierte Frameworks wie Java- und .Net eingesetzt.

Das Karma der Teilnehmer

Bei den Editoren zum Verfassen von Beiträgen erwarten die Benutzer einerseits Formatierungsmöglichkeiten, andererseits ist die Eingabe von HTML-Code weder benutzerfreundlich noch unter Sicherheitsaspekten verantwortbar. Die meisten Systeme setzen eine Markup-Sprache namens BBCode für typische Formatierungen (fett, kursiv) ein. Für darüber hinausgehende Funktionen kocht letztendlich jedes Forensystem sein eigenes Süppchen. Neben den Auszeichnungen, die sich unmittelbar in HTML-Markup übersetzen lassen, gibt es Funktionen wie die oben bereits erwähnte Zitatfunktion; viele Systeme erlauben zudem die Definition eigener Markups: Einige Forensysteme bieten komplette WYSIWYG-Editoren an.

Unter Umständen kann es sinnvoll sein, den Teilnehmern zusätzliche Funktionen neben dem eigentlichen Diskutieren zur Verfügung zu stellen. Beliebt ist die Möglichkeit, Umfragen hinzuzufügen. Mitglieder können zwischen den vorgegebenen Antworten wählen – das System übernimmt die Zählung und grafische Auswertung der Stimmen. Viele Systeme erlauben es, Dateien an einen Beitrag zu hängen. Welche Dateiformate und -größen erlaubt sind, lässt sich in der Regel in der Administrationsoberfläche konfigurieren.



punBB mag es minimalistisch – Funktionen zum Erstellen von Umfragen oder eine BBCode-Toolbar sucht man vergebens (Abb. 1).

Da Webforen immer auch ein Ort der Selbstdarstellung sind, können User bei Bedarf dem eigenen Profil Avatare zuordnen. Über Ranking-Systeme kann die Aktivität eines Benutzers im Forum aufgezeigt werden; manche Foren bieten auch an, einzelne Posts oder Threads zu bewerten. Höher bewertete Threads sorgen für ein besseres Ranking in Übersichtsseiten und steigern das Karma des Diskutanten.

Der Mehrwert eines Forums besteht darin, der Allgemeinheit Meinungen und Kenntnisse kundzutun. Trotzdem sind in manchen Situationen direkte, von der Öffentlichkeit unbemerkte Nachrichten zwischen Forenteilnehmern hilfreich.

Bei diesem Private Messaging (PM) landen die Nachrichten in einer foreninternen Mailbox; der Empfänger kann sich bei neuen Nachrichten durch E-Mail informieren lassen. Neben diesen PM kann der Teilnehmer Abonnements anlegen, um über neue Forenbeiträge informiert zu werden; wahlweise bei allen neuen Beiträgen in einem Forum oder nur bei Antworten auf eigene Beiträge. Dabei verhalten sich alle vorgestellten Systeme intelligent genug, die User nicht zuzuspammen, sondern nur eine Benachrichtigung bis zum nächsten Besuch zu versenden.

Forensysteme sind in ihrer Bedienung und Anwendung im hohen Maße standardisiert; die Grundfunktionen eines Forums lassen sich mit modernen Entwicklungswerkzeugen schnell selbst entwickeln. Wer so etwas vorhat, sollte aber wissen, dass diese Standardisierung eine entsprechende Erwartungshaltung von Benutzern, Moderatoren und Administratoren zur Folge hat. Zwar fängt man in der Regel klein an und posted und moderiert nach Leibeskräften selber. Wenn aber endlich die kritische Masse erreicht ist und das Forum prominent ist, können oder müssen weitere Moderatoren die Arbeit übernehmen. Spätestens dann sind ausgereifte Pflegewerkzeuge vonnöten und der Einsatz eines „professionellen“ Systems ist zu empfehlen.



punBB

Ein verbreitetes Forensystem ist punBB, weil es vor allem besonders einfach und genügsam ist. Es hat den Anspruch, sich auf die wesentlichen Funktionen eines Forums zu beschränken, was sich in der Standardinstallation widerspiegelt. Features wie das Splitten von Beiträgen, Datei-Uploads oder Umfragen sucht man hier vergeblich; eine Toolbar zum Formatieren der Beiträge fehlt ebenso. Allerdings gibt es dank der Popularität von punBB eine große Anzahl von Erweiterungen und Themes.

punBB erlaubt die Integration von Admin-Plug-ins, eine einfache Methode, neue Funktionen in die Administrationsoberfläche zu integrieren. Funktionen im Frontend hingegen werden über sogenannte Mods eingebunden. Dabei handelt es sich im Wesentlichen um eine Beschreibung, wie und an welchen Stellen der Original-Sourcecode zu erweitern ist: Ein aufwendiger, aber überschaubarer Vorgang.

Kompliziert wird es hingegen beim Update. Sollen bisherige Modifikationen erhalten bleiben, empfiehlt sich ein Update der Software über die vom Entwickler zur Verfügung gestellten *diffs*: Ein Prozess der wohl nur eingefleischten Unix-Admins leicht von der Hand geht. Alle anderen müssen eben die Modifikationen bei jedem Update von Hand nachziehen.

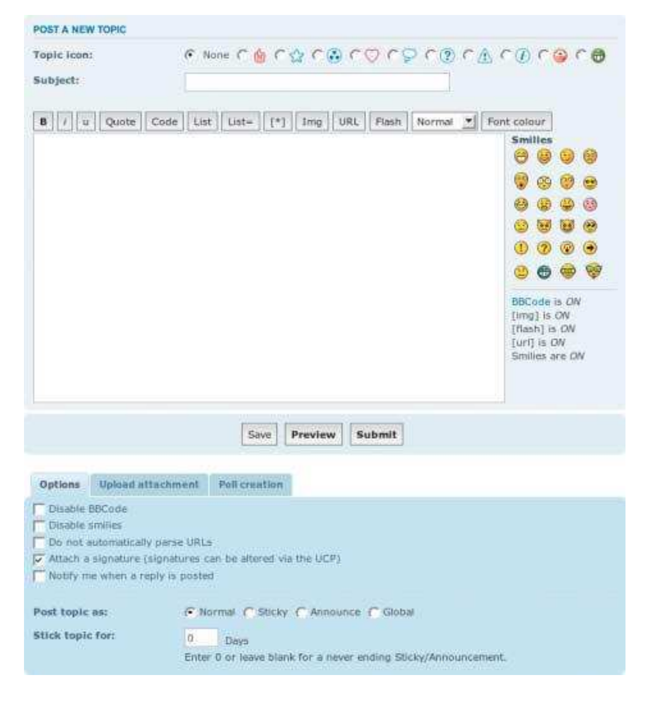
Das in PHP geschriebene punBB ist GPL-lizenziert und speichert seine Daten wahlweise in einer MySQL-, PostgreSQL- oder SQLite-Datenbank.



phpBB

phpBB ist wohl das populärste Open-Source-Forum. Erst im Dezember erschien die neue Version 3.0 – Sourcecode und Features sind komplett überarbeitet. Wie der Name andeutet, ist phpBB in PHP geschrieben und unterstützt zur Datenspeicherung mit MySQL, PostgreSQL, SQLite, Firebird, Microsofts SQL Server und Oracles RDBMS eine große Auswahl an Datenbanken.

Neben dem neuen, moderneren Design haben die Entwickler viele bisher nur als Add-on verfügbare Features der Standardinstallation hinzugefügt. Dazu gehören unter anderem selbst konfigurierbare BBCodes, Datei-Uploads,



phpBB geizt nicht mit Optionen und Schaltflächen beim Erstellen eines Postings: BBCode, Smileys, Dateianhänge und Umfragen lassen sich über die Oberfläche einbinden (Abb. 2).

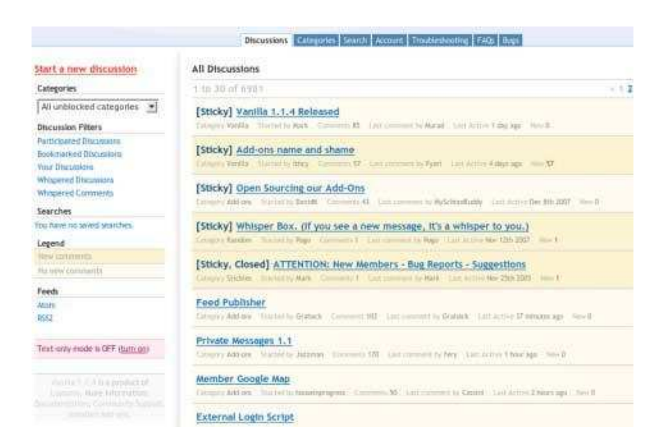
integriertes Caching sowie verbesserte Moderationsmöglichkeiten. Zudem setzt phpBB komplett auf UTF-8 als Zeichensatz. Unerklärlich hingegen ist, warum man auf die Unterstützung von RSS-Feeds verzichtet hat.

Mussten bisher Add-ons von Hand in den Sourcecode eingepflegt werden, unterstützt die neue Version ein „Hook“-System, das Plug-ins ohne Core-Modifikationen in die Applikation integriert. Durch den kürzlichen Versionssprung sind viele Themes und Addons noch nicht kompatibel mit dem neuen System, dennoch stehen bereits jetzt viele Erweiterungen zur Verfügung: bei – nach eigenen Angaben – mehreren Millionen Installationen ist die Entwicklergemeinde eben entsprechend groß.

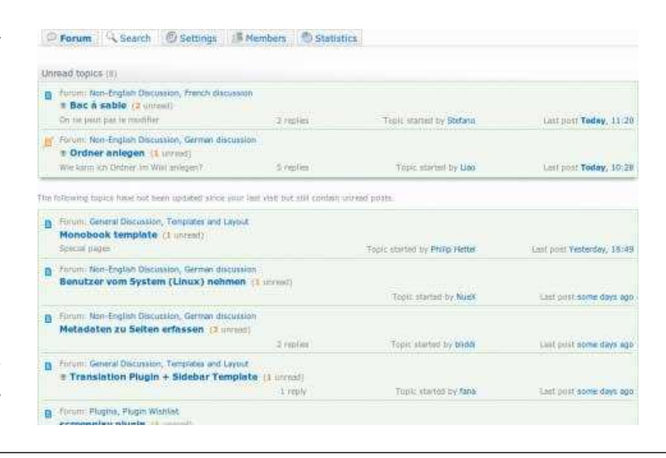


Vanilla

Vanillas erstes Release wurde 2005 vorgestellt und traf damit genau die entstehende Web-2.0-Welle. Statt wie andere Foren auf der Startseite eine Übersicht der verschiedenen Kategorien zu geben, begrüßt einen Vanilla gleich mit den



Vanilla stellt die aktuellen Diskussionen in den Vordergrund und verbannt die klassische Kategorienansicht von der Startseite (Abb. 3).



Das Unclassified Newsboard überzeugt mit durchdachten Funktionen. Hier die Ansicht der ungelesenen Posts (Abb. 4).

Forensysteme								
Produkte	**phpBB**	**punBB**	**vBulletin**	**JForum**	**UNB**	**Vanilla**	**Burning Board**	**YetAnotherForum.NET**
URL	phpbb.com	punbb.org	vbulletin.com	jforum.net	newsboard.unclassified.de	getvanilla.com	woltlab.de/products/burning_board/	yetanotherforum.net
Lizenz	GPL	GPL	proprietär	BSD	GPL	GPL	proprietär	GPL
Kosten	keine	keine	79 €/Jahr, 149 € Vollversion	keine	keine	keine	50–200 €, kostenlose „Light"-Version	keine
UTF-8-Support	ja	nein	nicht per default	ja	ja	ja	ja	ja
Datenbank	MySQL, PostgreSQL, Oracle, Firebird, SQLite	MySQL, PostgreSQL, SQLite	MySQL	MySQL, PostgreSQL, Oracle, HSQLDB, MS SQL Server	MySQL	MySQL	MySQL	MS SQL Server
Programmiersprache	PHP	PHP	PHP	Java	PHP	PHP	PHP	C# und ASP.Net
Struktur/Typ	flach	flach	flach/threaded	flach	flach	flach	flach	flach/threaded
verschachtelte Subforen	unbegrenzt	nein	unbegrenzt	nein	unbegrenzt	nein	unbegrenzt	ja
Moderation								
Split Thread	ja	nein	ja	nein	ja	nein	ja	nein
Sticky Thread	ja	ja	ja	ja	ja	ja	ja	ja
Close Thread	ja	ja	ja	ja	ja	ja	ja	ja
Customizing								
Templates	ja	ja	ja	ja	ja	ja	ja	ja
Skin-Editor	ja	nein	ja	nein	nein	nein	ja	nein
Plug-ins	ja	nein (nur Admin-Interface)	ja	nein	ja	ja	ja	nein
Security								
IP-Block	ja	ja	ja	ja	nein	nein	ja	ja
Ban User	ja	ja	ja	ja	ja (über Gruppen-mitgliedschaft)	ja	ja	ja
Flood Control	ja	ja	ja	ja	ja	ja	ja	ja
Captcha	ja	nein	ja	ja	ja	nein	ja	nein
Administration								
Groups	ja	ja	ja	ja	ja	ja	ja	ja
ACL	ja	nein	ja	ja	ja	ja	ja	ja
LoFi View	ja	nein	ja	nein	nein	nein	nein	nein
Funktionen für die Teilnehmer								
Rating/Karma	nein	nein	ja	ja	nein	nein	ja	nein
Umfragen	ja	nein	ja	ja	ja	nein	ja	ja
Unread Topics	post	visit	post	visit	post	post	post	visit
Custom BBCode	ja	nein	ja	ja	nein	nein (HTML erlaubt)	nein	
WYSIWYG/BBCode Toolbar	Toolbar	nein	Toolbar	Toolbar	Toolbar	nein	WYSIWYG	Toolbar
Private Messaging	ja	nein	ja	ja	ja	ja (whispering)	ja	ja
Dateianhänge	ja	nein	ja	ja	ja	ja	ja	ja
RSS/ATOM	nein	ja	ja	ja	ja	ja	ja	ja

Datenbanken: Bei der Oracle-Datenbank beziehungsweise beim MS SQL Server reicht die jeweilige kostenlose Express-Version.

aktuellen Diskussionen – egal aus welcher Kategorie. Der Fokus wird also, ganz Web 2.0, bewusst auf die Benutzerbeiträge gelegt. RSS-Feeds kann Vanilla nicht nur für das ganze Forum oder einzelne Kategorien, sondern auch für einzelne Threads ausliefern.

Auch Vanillas Extension System erlaubt das Erweitern des Systems ohne Core-Modifikationen. Während es eine relativ große Auswahl an fertigen Plugins gibt, ist die Anzahl der verfügbaren Themes eher begrenzt.

Ein besonderes Feature ist das „Whispering". Es erlaubt das „Flüstern" von Posts nur an einem bestimmten Diskutanten: Private Messaging im Web 2.0. Ein derartiger Post fügt sich ganz normal in den Diskussionsfluss ein, aber nur direkt Angesprochene können ihn sehen. Mittels dieser Methode kann man beispielsweise Kommentare abgeben, ohne einen Flamewar gleich wieder anzuheizen.

Erwähnenswert ist zudem, dass Vanilla den Titel eines Diskussionsstrangs in die URL integriert – Suchmaschinen belohnen solche sprechenden URLs. Vanilla setzt wie viele andere Systeme auf PHP und MySQL auf. Der Code steht unter der GPL-Lizenz.



Unclassified Newsboard

Unclassified NewsBoard (UNB) ist ein noch relativ unbekanntes Open-Source-Forensystem. Es setzt auf die Kombination aus PHP und MySQL. Hauptaugenmerk legten die Entwickler darauf, dass direkt nach der Installation ein mit allen typischerweise benötigten Features ausgestattetes System vorliegt. Neben Moderationswerkzeugen, einer BBCode Toolbar, Umfragen, File Uploads und RSS Support gehören weniger häufige Features wie integrierte Statistiken, Bookmarking und Benachrichtigungen über Jabber zum Standardfunktionsumfang. Nutzer schätzen vor allem den individuellen Lesestatus für jeden Post.

Zudem erlaubt UNB beliebig tief verschachtelte Subforen, besonders große oder mehrsprachige Communities profitieren davon. Zusätzlich zum Markieren von Posts als „sticky" können Moderatoren in jedem Forum „Announcements" posten, die auf Wunsch auch in Subforen zu sehen sind. Ein komplexes ACL-Management erlaubt es, einzelne Forenrechte detailliert zu

konfigurieren – vordefinierte Rechte (Mitglied, Moderator, Administrator) vereinfachen den Einstieg.

Erwähnenswert ist der durchgängige UTF-8-Support; leider noch keine Selbstverständlichkeit bei Forensystemen. Über Themes und Plug-ins kann man das Forum erweitern und anpassen, ohne Modifikationen am Corecode vornehmen zu müssen. Abstriche muss man jedoch bei der Anzahl der bereits verfügbaren Plug-ins und Themes machen. Neben dem deutsch- und englischsprachigen Supportforum gibt es Business-Support auch direkt vom Entwickler.



vBulletin erlaubt neben der dominierenden flachen Ansicht auch das Einblenden der Diskussionsstränge in einem Threaded View (Abb. 5).

Woltlabs Burning Board ermöglicht die Formatierung von Posts über den integrierten WYSIWYG-Editor (Abb. 6).



vBulletin

vBulletin setzt ebenfalls auf PHP und MySQL, wird aber anders als die bisher vorgestellten Systeme nicht unter einer Open-Source-Lizenz vertrieben. Dennoch erfreut es sich großer Beliebtheit und gilt vielen Open-Source-Foren als Vorbild.

Die hinter vBulletin stehende Firma Jelsoft Enterprises Ltd. bietet zwei unterschiedliche Lizenzmodelle an. Beim Kauf einer Vollversion erhält man ein Jahr lang kostenlose Updates und kann die Software unbegrenzt lange einsetzen. Als Alternative gibt es die preiswertere Einjahreslizenz, die man als Betreiber allerdings jedes Jahr erneuern muss. Beide Lizenzen enthalten kostenlosen E-Mail-Support.

vBulletin bietet eine Vielzahl von Features, die man in anderen Foren erst über Plug-ins oder Erweiterungen nachrüsten muss. Die dazugehörigen Konfigurationsoptionen erfordern zwar einigen Aufwand, machen vBulletin aber letztlich flexibel anpassbar.

Sollten dennoch Funktionen fehlen, kann man Erweiterungen über das vorhandene Plug-in-System installieren, Quellcode-Änderungen bleiben einem so erspart. Das Aussehen lässt sich über die Installation von Templates anpassen. Kleinere Designänderungen können über den integrierten Style-Editor vorgenommen werden. Eigene BBCodes lassen sich ebenfalls im Administrations-Backend definieren. Administratoren großer Foren dürften vor allem die für Suchmaschinen optimierte LoFi-Archivansicht schätzen.

Derzeitiges Manko ist die standardmäßig nicht aktivierte UTF-8-Unterstützung. Nur wer weiß, wie es geht, kann vBulletin mit UTF-8 betreiben [c]. Erst die Version 4.0 soll dies ändern.



Burning Board

Das Burning Board der Berliner Firma Woltlab erfreut sich nicht nur in Deutschland großer Beliebtheit. Im Dezember letzten Jahres erschien Version 3, die einige neue Features einführte. Das System bietet, ähnlich wie Vanilla, „Speaking URLs“ und unterstützt die Erweiterung des Systems durch Plug-ins. UTF-8 wird jetzt als durchgängiges Encoding verwendet.

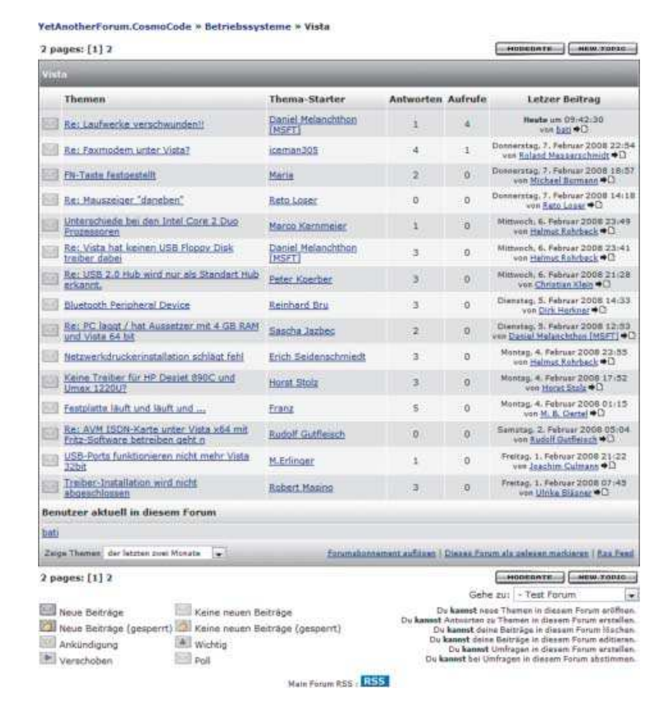
Anders als die meisten anderen Foren setzt Woltlab auf einen WYSIWYG-Editor und macht den aus anderen Foren bekannten BBCode damit überflüssig. Typische Forenfeatures wie Datei-Uploads und Umfragen liefert das System gleich mit. Andere Erweiterungen kann der Betreiber über ein Plug-in-System ohne Core-Modifikationen nachinstallieren.

Besonderes Augenmerk wurde bei der Entwicklung der neuen Version auf die Barrierefreiheit gelegt. Burning Board ist eines der wenigen Foren, die komplett auf Tabellen für das Seitenlayout verzichtet.

Woltlab bietet neben der reinen Software-Lizenz auch Pakete mit zusätzlichen Support- und Upgrade-Verträgen



Per Lesezeichen, wie hier beim JForum, behält man interessante Diskussionen einfacher im Blickfeld. Sie können zudem für andere Forenbenutzer über das eigene Profil sichtbar sein (Abb. 7).



Newsgroups von NNTP-Servern lassen sich beim YetAnother Forum.NET nahtlos in das eigene Forum einbinden. Antworten auf diese Diskussionen gelangen jedoch (noch) nicht zurück zur Usenet-Quelle (Abb. 8).

an. Eine kostenlose Burning-Board-Lite-Version ist ebenfalls erhältlich, hier muss man allerdings auf Features wie den WYSIWYG-Editor verzichten.



JForum

JForum ist eine in Java programmierte Software, die mit Stabilität und Geschwindigkeit wirbt. Sie ist frei verfügbar und steht unter der BSD-Lizenz. JForum läuft auf Anwendungsservern wie Tomcat, JBoss und Resin, unter Java EE 5 SDK. Bei den Datenbanken gibt man sich freizügig: Neben MySQL, PostgreSQL und Oracle werden Microsoft SQL Server und HSQLDB unterstützt.

Das stark an phpBB (Version 2) angelehnte Aussehen und die Positionierung der Elemente erleichtert einen Umstieg auf JForum; zudem wird ein Migrationstool angeboten, das den Datenbestand aus phpBB oder PHPNuke migriert.

Leider fehlt eine Plug-in-API zur Erweiterung des Forums um eigene Funktionen – dafür ist die Integration des Forums selbst in andere Anwendungen möglich. Der Kontext der Applikation ist über das Java-Konzept Threadlocal identifizierbar. JForum bietet zudem Support für Single-Sign-On über Login-Cookies oder Authentifizierungs-Frameworks. Die Authentifizierung lässt sich außerdem an LDAP- oder einen Directory-Server delegieren.

Das von JForum verwendete, Velocity ähnliche Template-System Freemarker ermöglicht eine vielseitige Anpassung. Selbst eine komplette Umstrukturierung des gesamten Seitenaufbaus ist möglich. Für Administratoren gibt es ein umfangreiches ACL-System. Nützlich für Benutzer: Lesezeichen von Threads können gespeichert und anderen Forenbesuchern zugänglich gemacht werden.



YetAnotherForum.Net

YetAnotherForum.Net (YAF) ist eines der wenigen Foren, das auf Microsofts ASP.Net setzen. Wer sich für dieses System entscheidet, erhält ein Paket mit den üblichen Forenfunktionen. Zwar lässt sich, wie bei allen anderen vorgestellten Systemen, die Sprache des Forums über Sprachdateien anpassen, der Adminbereich unterstützt aber keine Mehrsprachigkeit und bleibt daher Englisch.

Das Aussehen lässt sich über editierbare CSS und austauschbare Buttons beziehungsweise Symbole anpassen, die zusammen ein Theme bilden. Ein Skin-Editor ist nicht im Installationsumfang enthalten. Man kann jedoch jedem Subforum ein eigenes Theme zuordnen und ihm damit ein individuelles Aussehen verpassen.

Eine neue Funktion (momentan noch Beta) bietet die Möglichkeit, Newsgroups von NNTP-Servern einzubinden. So lassen sich Artikel aus dem Usenet in ein Subforum integrieren. Antworten auf diese Artikel werden jedoch nicht zurück ins Usenet gespeist. YAF lässt sich zudem in die .Net-Applikationen DotNetNuke und Rainbow integrieren, im ASP.Net Umfeld bekannte Systeme zur Erstellung von Webportalen.

Der komplett in C# geschriebene Sourcecode ist unter der GPL-Lizenz verfügbar. Zur Datenspeicherung wird ein Microsoft SQL Server (Express) ab der 2000er-Generation benötigt.

Fazit

Forensysteme sind im Web etablierte und stabile Kommunikationsplattformen. In der Handhabung sind die Systeme weitestgehend standardisiert, das Aussehen damit leider auch: Einzig Vanilla punktet mit einem modernen GUI.

Wer etwas Besonderes will, muss Hand anlegen. Viele Systeme bieten für gestalterische Anpassungen die nötigen Werkzeuge. Wer bereits PHP und MySQL auf seinem Server im Einsatz hat, findet für diese Kombination die größte Auswahl.

Soll der Funktionsumfang der geplanten Community über die Features der eingesetzten Software hinausgehen, empfiehlt es sich, bei der Auswahl auf eine ausgereifte Plug-in-Architektur zu achten. (WM)

DETLEF HÜTTEMANN

ist CEO der Berliner CosmoCode GmbH. Das Softwarehaus entwickelt individuelle Internetlösungen für den Mittelstand und betreibt unter anderen die Vergleichsportale ForumMatrix und WikiMatrix.

ANDREAS GOHR

ist Angestellter bei CosmoCode und unter anderem Entwickler der Open-Source-Software DokuWiki.

TILO BALLER

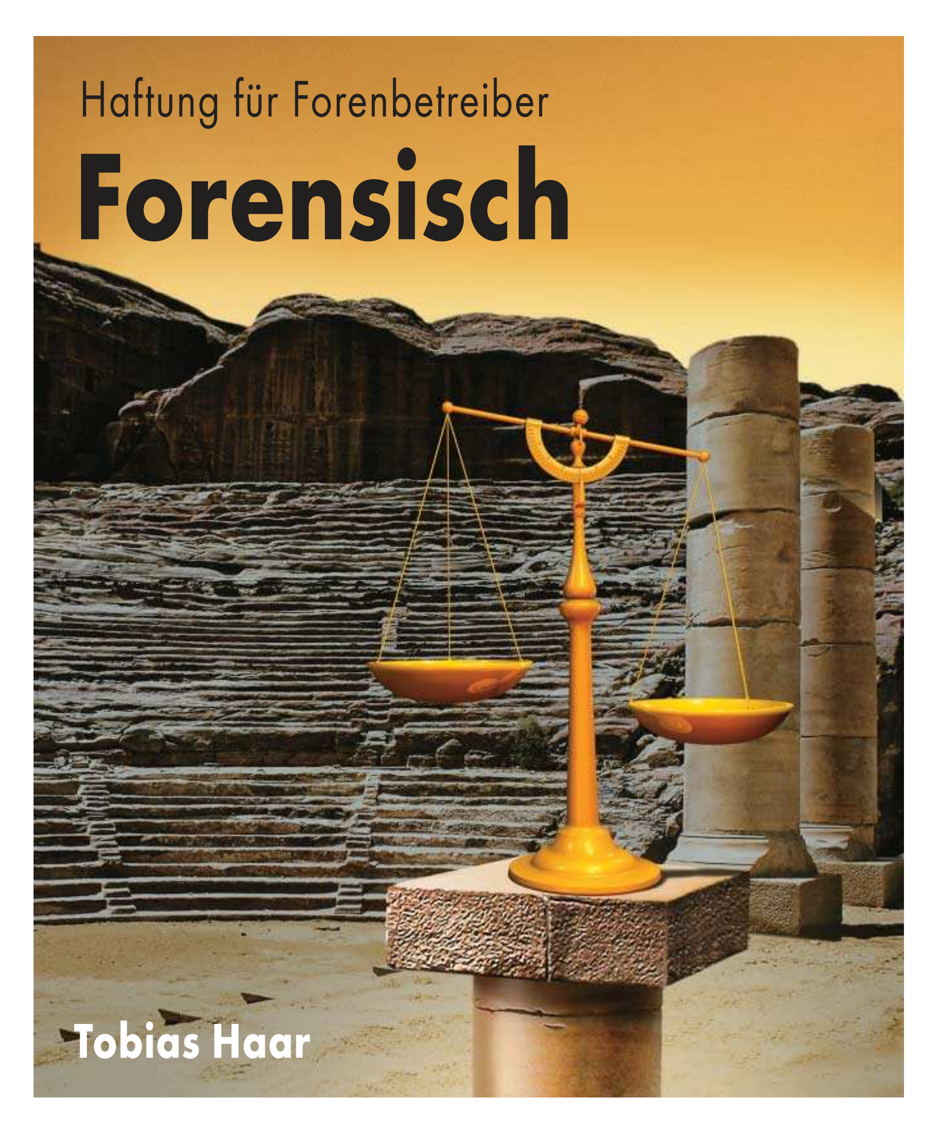
ist Auszubildender bei CosmoCode und im Bereich PHP-Entwicklung tätig.

Onlinequellen

[a] Online-Übersicht über Forensoftware
www.forummatrix.org

[b] Pflicht zur Löschung von Beiträgen
www.heise.de/newsticker/meldung/72026

[c] UTF-8 für vBulletin
www.vcharset.com/how-to-start-vbulletin-forum-with-utf-8-from-the-begining-pid4.html



Haftung für Forenbetreiber
Forensisch

Tobias Haar

Kaum eine Rechtsfrage bewegt die Gemüter der Betreiber von Onlinediensten mehr als die nach der Haftung für fremde Inhalte. Gerade die Anbieter von Meinungs- und Diskussionsforen sowie Blogs im Internet bewegen sich hier rechtlich auf dünnem Eis, wenn sie nicht entsprechende Vorsichtsmaßnahmen ergreifen.

Der Laie staunt, der Fachmann wundert sich. Zugegeben, es ist nicht leicht zu verstehen, dass es Meldungen über Urteile wie „Keine Überwachungspflichten für Forenbetreiber“ und nur kurze Zeit später „Urteil bestätigt uneingeschränkte Haftung für Forenbetreiber“ gibt. Eigentlich sind es nur vier Paragrafen im Telemediengesetz, dem früheren Teledienstegesetz, die seit Jahren zu unzähligen Urteilen, aber nicht zwingend zu einer eindeutigen und immer nachvollziehbaren Rechtslage in diesem Bereich geführt haben.

Nicht zuletzt der Heise-Verlag musste in dieser Hinsicht (unfreiwillig) seine Erfahrungen machen, als es um die Frage ging, ob er Forenbeiträge vor ihrer Freischaltung auf die rechtliche Zulässigkeit ihres jeweiligen Inhalts zu überprüfen hat. Also im konkreten Fall, ob man den Verlag als Anbieter eines Internetforums für einen unzulässigen Beitrag eines Nutzers zur Verantwortung ziehen kann.

In erster Instanz war er mit der Begründung verurteilt worden, er könne ja die Foren so gestalten, dass „die Einträge vor ihrer Freischaltung auf die rechtliche Zulässigkeit ihres jeweiligen Inhalts überprüft werden“. Das Gericht verlangte somit eine Vorabprüfung sämtlicher Beiträge. Für größere Foren ein sehr aufwendiges und teures Prozedere. Im Berufungsverfahren relativierte das Gericht diese Pflicht dann ein wenig. Die Vorabprüfungspflicht gilt nur eingeschränkt, aber es gibt sie eben in bestimmten Fällen. Wann genau, das ist die noch immer in Diskussion befindliche Frage.

Am Anfang war die Beleidigung

Rechtliche Auseinandersetzungen im Bereich von Internetforen beginnen nahezu immer damit, dass sich jemand durch eine Äußerung in einem Forum in seinen Rechten verletzt fühlt. Ein solchermaßen Verletzter hat grundsätzliche mehrere Ansprüche, die er geltend machen kann. Zum einen hat er ein Interesse daran, dass die rechtswidrigen Äußerungen schnell aus dem Forum verschwinden und auch nicht wiederholt werden. Zum anderen möchte er für einen erlittenen materiellen oder immateriellen Schaden entschädigt werden. Er wird also die Geltendmachung von Schadenersatz und Schmerzensgeld in Erwägung ziehen.

Grundsätzlich haftet der Autor einer rechtswidrigen Äußerung gegenüber dem Verletzten. Wer jemanden beleidigt, muss ihm gegenüber dafür geradestehen. So die Theorie. In Internetforen ist es aber regelmäßig so, dass der Betroffene die Forennutzer nicht ohne Weiteres ausfindig machen kann, da diese ihre Beiträge meist unter Pseudonymen veröffentlichen. Daher bleibt ihm zunächst nur das Vorgehen gegen den Betreiber des Forums. Für diesen Diensteanbieter gelten jedoch die besonderen Haftungsregelungen nach dem Telemediengesetz. Bevor zu entscheiden ist, ob nach sonstigen Vorschriften überhaupt eine rechtswidrige Äußerung vorliegt, muss nach diesen Regelungen als eine Art „Filter“ vorab geprüft werden. Übrigens darf sich nach einem Urteil des Bundesgerichtshofs ein Verletzter auch dann an den Blogger oder Forenbetreiber halten, wenn ihm die Identität des Autors bekannt ist.

Die genannten „Filterregeln“ lassen sich in zwei Gruppen einteilen. Da ist zum einen die Haftung für eigene Äußerungen und zum anderen die für Äußerungen Dritter, die man sich aber – aus welchen Gründen laut Telemediengesetz auch immer – zurechnen lassen muss. § 7 Absatz 1 des Telemediengesetzes sagt eindeutig zur ersten Fallgruppe: „Diensteanbieter sind für eigene



Bei gut frequentierten Foren ist die Kontrolle der Beiträge ein aufwendiges und kaum zu bewältigendes Unterfangen. Bei heise online etwa fallen täglich 5000 bis 6000 neue Forumsbeiträge an.

Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.“ Der Content-Provider, wie beispielsweise beim Internet-Auftritt eines Zeitschriftenverlages, ist demnach für die Inhalte seiner Webseiten selbst verantwortlich. Das leuchtet ein. Von diesen sind die Access-Provider, die Zugang etwa zum Internet vermitteln, und die Host-Provider, die fremde Inhalte für den Nutzer speichern, abzugrenzen. So weit, so gut.

Verschiedene Arten der Verantwortung

Ein Forenbetreiber haftet also für die von ihm selbst eingestellten Forenbeiträge in vollem Umfang. Das gilt ebenfalls für die seiner Mitarbeiter, etwa, wenn es sich um ein moderiertes Forum handelt. Denn dann muss sich der Betreiber das Verhalten seiner Mitarbeiter als eigenes zurechnen lassen. Auch der zweite Fall, der Access-Provider, ist noch relativ leicht zu fassen. Wer die Kommunikation nicht veranlasst, die Adressaten von Informationen und auch die Informationen nicht ausgewählt hat, ist für rechtswidrige Inhalte, zu denen nur der Zugang vermittelt wird, nicht verantwortlich.

Damit sind die Internet-Service-Provider wie T-Online, Arcor, Freenet und alle anderen von der Haftung befreit, soweit sie nicht eigene Webangebote und nur den „Internetzugang“ zur Verfügung stellen. Diese Haftungsfreistellung gilt übrigens auch für Betreiber von Proxy-Servern, die automatisch und kurzfristig fremde Informationen zwischenspeichern.

Dem Forenbetreiber hilft aber die Haftungsprivilegierung des Access-Providers nicht weiter, denn er wird in der Regel als Host-Provider angesehen. Für diese gilt nach § 10 Telemediengesetz, dass sie für „fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich“ sind, wenn „sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadenersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird“.

Sie sind auch dann nicht verantwortlich, wenn „sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben“. Anderenfalls haften sie gegenüber den Verletzten und können gleichfalls schadenersatzpflichtig sein oder unter Umständen sogar strafrechtlich zur Verantwortung gezogen werden, etwa wegen Beleidigung. Mit anderen Worten: Wenn sie auf eine beleidigende Äußerung hingewiesen werden, sollten sie diese schnell löschen.

Sonderfall Vorabkontrolle

Eine Besonderheit ergibt sich aus einem Urteil des Bundesgerichtshofes (Urteil vom 11.02.2004, Az. 324 O 794/07). Dieser entschied, dass die Vorschriften des Telemediengesetzes auf Unterlassungsansprüche keine Anwendung finden. Verlangt also ein in seinen Rechten Verletzter neben der sofortigen Löschung auch die Unterlassung der Wiederholung einer rechtswidrigen Äußerung in einem Forum von dessen Betreiber, besteht ein solcher Anspruch unabhängig von der Kenntnis des Forenbetreibers immer dann, wenn dieser eine Vorabkontrollpflicht hatte und sie im konkreten Fall verletzt hat.

Das Landgericht Hamburg (Urteil vom 04.12.2007, Az. 324 O 794/07) hat für diese Pflicht des Weblog-Betreibers einen sogenannten „gleitenden Sorgfaltsmaßstab“ und ein „Spektrum abgestufter Prüfpflichten“ definiert. Das bedeutet, dass der Betreiber einer Vorabkontrollpflicht dann unterliegt, wenn dafür ein konkreter Anlass gegeben ist. Die Richter äußerten sich noch etwas genauer: „Je mehr konkreter Anlass zu der Befürchtung besteht, dass es durch Kommentare auf einer Internetseite zu Persönlichkeitsrechtsverletzungen Dritter kommen wird, und je schwerwiegender die zu befürchtenden Verletzungen sind, umso mehr Aufwand muss der Betreiber auf sich nehmen, um die auf seiner Seite eingestellten Kommentare einer persönlichkeitsrechtlichen Überprüfung zu unterziehen“.

Ein solcher Anlass kann zum Beispiel vorliegen, wenn eine rechtswidrige Äußerung eines Nutzers absehbar ist. In diesem Fall war das nach Auffassung der Richter so, denn der Beklagte hatte selbst einen scharfen, kritischen Artikel auf seiner Webseite eingestellt, den ein Nutzer seines Blogs in beleidigender Weise kommentiert hatte. Gegen diesen Kommentar richtete sich das Gerichtsverfahren. Da der Blog-Betreiber also selbst die ehrverletzenden Äußerungen durch Nutzer provoziert hatte, traf ihn eine Vorabkontrollpflicht, die er verletzt hatte.

Ähnlich hatte auch das Oberlandesgericht Hamburg im „Heise-Fall“ (Urteil vom 22.08.2006, Az. 7 U 50/06) entschieden. Dort verlangten die Richter eine Vorabkontrolle aller Beiträge zu einem Diskussionsthema in einem Forum durch den Betreiber, „wenn dieser entweder durch sein eigenes Verhalten vorhersehbar rechtswidrige Beiträge Dritter provoziert hat oder wenn ihm bereits mindestens eine Rechtsverletzung von einigem Gewicht im Rahmen des betreffenden Forums benannt worden ist und sich damit die Gefahr weiterer Rechtsverletzungen durch einzelne Nutzer bereits konkretisiert hat“. Außerdem führte das Gericht aus, dass einem gewerblichen Betreiber eine laufende Überwachung der Meinungsbeiträge eher zuzumuten ist als einem privaten.

Man hätte es ahnen können

In anderen Fällen haben Gerichte eine Kontrollpflicht etwa dann angenommen, wenn dem Betreiber früher bereits mindestens einmal eine gewichtige Rechtsverletzung zur Kenntnis gelangt ist und er deswegen davon ausgehen muss, dass die Nutzer des Blogs oder Forums zu solchen Rechtsverletzungen bereit sind.

Wird durch eine Vorabkontrolle oder durch einen Hinweis oder die Aufforderung eines Dritten ein rechtswidriger Beitrag identifiziert, ist dieser unverzüglich aus dem Blog oder Forum zu entfernen. Damit hat man der rechtlichen Pflicht Genüge getan. Man darf sich als Betreiber darauf verlassen, dass Suchmaschinenbetreiber ihre Datenbestände regelmäßig aktualisieren. Eine Pflicht, von diesen aktiv eine Löschung der Auflistung des (gelöschten) rechtswidrigen Beitrags zu verlangen, besteht nicht.

Wer seine Prüfpflichten verletzt, kann auf Beseitigung der rechtswidrigen Beiträge und Unterlassung der Wiederholung einer solchen Äußerung in Anspruch genommen werden. Im Wiederholungsfall hat er meist ein vom Gericht festgesetztes Ordnungsgeld von bis zu 250 000 Euro zu zahlen. Theoretisch kann ein Gericht auch Ordnungshaft gegen den Verantwortlichen – etwa den Geschäftsführer einer GmbH – anordnen. Solche Fälle sind aber extrem selten. Gerade die Möglichkeit, im Wiederholungsfall mit Ordnungsgeld belegt zu werden, ist das eigentliche kostspielige Risiko. Denn dieses resultiert automatisch daraus, dass der Betreiber künftig jeden Forenbeitrag daraufhin durchsehen muss, ob jemand die abgemahnte Äußerung wiederholt.

Usenet-Betreiber unterliegen übrigens nicht dieser Vorabkontrollpflicht. Denn sie sind eher mit einem Access-Provider zu vergleichen, für den diese Grundsätze nicht gelten. Das meinten jedenfalls die Richter am Oberlandesgericht Düsseldorf (Urteil vom 15.01.2008, Az. I-20 U 95/07). Denn, so ihr Urteil, dem Provider muss eine Kontrolle überhaupt möglich, zumindest aber zumutbar sein. Dies ist beim Usenet-Betreiber aber nicht der Fall, denn er ist nicht in der Lage, „rechtsverletzende fremde Inhalte aus dem Usenet zu löschen“. Nur von seinem eigenen Server kann er solche Beiträge löschen, bis diese erneut von einem Usenet-Nutzer abgerufen und dort abgelegt werden.

Fazit

Betreiber von Blogs und Meinungsforen tun gut daran, sich mit ihrer Haftung für rechtswidrige Beiträge durch Dritte zu beschäftigen. Die deutschen Gerichte erwarten eine Vorabkontrolle der Beiträge zumindest dann, wenn mit rechtswidrigen Äußerungen zu rechnen ist. Das ist der Fall, wenn durch das diskutierte Thema rechtswidrige Beiträge naheliegen oder durch andere Beiträge – insbesondere von den Betreibern selbst eingestellte Artikel – geradezu provoziert werden.

Viele Forenbetreiber schützen sich dadurch, dass sie entweder die Beiträge vorab oder jedenfalls unmittelbar nach ihrer Veröffentlichung auf rechtswidrige Inhalte kontrollieren. Manche benutzen dazu auch Filtersoftware, die neue Beiträge auf bestimmte Schlüsselwörter hin untersucht und diese dann entweder automatisch sperrt oder in einen Quarantänebereich ablegt, der manuell durch die Verantwortlichen zu überprüfen ist.

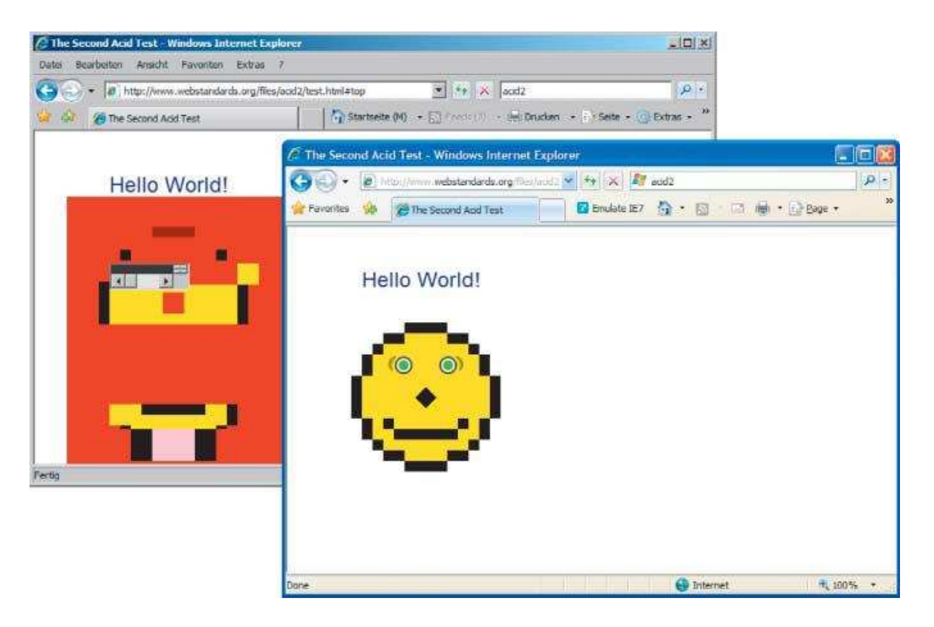
Problematisch ist daran, dass hier meist durch Laien eine juristische Prüfung der Beiträge erforderlich ist, die in rechtlichen Grauzonen auch misslingen kann. Letztlich wird also ein Betreiber lieber einen Artikel zu viel als einen zu wenig von der Veröffentlichung ausschließen. Ob das noch im Sinne der grundrechtlich geschützten Meinungs- und Pressefreiheit ist, darf man zu Recht bezweifeln. Aber solange der Gesetzgeber hier nicht für klare Regeln sorgt, bleibt den Gerichten nichts anderes übrig, als der bislang befolgten Rechtsprechung des Bundesgerichtshofs und anderer hoher Gerichte zu folgen. Aus Kostengründen haben auch schon Betreiber „Öffnungszeiten“ für ihre Meinungsforen festgelegt, außerhalb derer keine Kontrolleure zur Verfügung stehen. Postings sind daher auch nur in diesen Zeiten möglich.

Mittels vertraglicher Haftungsbeschränkungen sein eigenes Risiko in diesen Fällen zu reduzieren, dürfte keine Alternative sein. Dann müsste man mit jedem Nutzer und „Leser“ zunächst einen Nutzungsvertrag über den Blog oder das Forum schließen. Selbst in solchen geschlossenen Gruppen wären aber auch nur geringfügige Erleichterungen möglich, denn Haftungsklauseln in Standardverträgen gibt das deutsche Recht über allgemeine Geschäftsbedingungen enge Grenzen vor. (ur)

TOBIAS HAAR, LL.M.,

ist Rechtsanwalt mit Schwerpunkt IT-Recht.





Internet Explorer zwischen 7 und 8

Kernsanierung

Michael Jendryschik

Schon die erste Beta-Version des Internet Explorer 8 ist deutlich besser als sein Vorgänger, bleibt aber weit hinter der Konkurrenz zurück. Der fertige Browser soll CSS 2.1 voll unterstützen.

Als der Internet Explorer 7 im Oktober 2006 erschien, rief er unter Webentwicklern zwiespältige Reaktionen hervor. Der Microsoft-Browser hatte zwar viele Änderungen an der Benutzeroberfläche erfahren, war aber in Bezug auf Webstandards nicht viel mehr als eine Art längst überfälliger Bugfix voller alter und neuer Probleme und Fehler [1]. Mittlerweile steht der IE 8 in den Startlöchern, bei dessen Entwicklung Microsoft deutlich höhere Maßstäbe angelegt hat. Die Entwicklung des IE 8 begann im August 2007. Im Dezember erschienen die ersten Einträge über den neuen Browser im Weblog der IE-Entwickler. Die erste öffentliche Beta-Version richtet sich primär an Webentwickler und steht seit dem 5. März 2008 zur Verfügung.

IE 8 wartet mit zahlreichen neuen Erweiterungen auf, darunter sogenannte Activities und Webslices. Erstere sind kleine Zusatzfunktionen, die Betreiber einer Website anbieten und Nutzer bei Bedarf installieren. Auf diese Weise können Surfer komfortabel typische Aktionen per Kontextmenü durchführen, beispielsweise eine Anschrift bei einem Stadtplandienst nachschlagen oder Übersetzungsdienste ansteuern. Kopieren und Einfügen zwischen zwei Websites ist dadurch einfacher oder überflüssig. Beschrieben werden Activities in XML; das Nachladen erfolgt per Javascript.

Neues Gefühl: Innovation im IE

Webslices sind Ausschnitte einer Website, die Benutzer wie Newsfeeds abonnieren können. Sie erscheinen als eine Form von Lesezeichen in der Favoritenleiste und eignen sich dazu, komfortablen Zugang zu Informationen zu schaffen, beispielsweise Aktienkursen oder dem aktuellen Stand einer Ebay-Auktion. Welche Bestandteile einer Webseite als Webslices zur Verfügung stehen, beschreiben Entwickler mit *hSlice*, einer Abwandlung des Mikroformats *hAtom*. Überhaupt zeigt sich die Favoritenleiste in einem neuen Gewand und verwaltet neben Lesezeichen und Webslices Newsfeeds und die Browser History.

Auch die Adresszeile des Browsers hat sinnvolle Erweiterungen erfahren. So graut IE 8 die gesamte aufgerufene URL aus – mit Ausnahme der Top-Level-Domain, die dadurch in den Vordergrund rückt und deutlich erkennbar ist. Wie der Umgang mit Services aussehen kann, bei denen eine Subdomain Bestandteil der Adresse ist (beispielsweise script.aculo.us oder del.icio.us), muss die Zukunft zeigen. Nützlich ist darüber hinaus die Unterstützung mehrzeiliger URLs, ein häufiges Ärgernis in E-Mails, in denen umbrochene URLs häufig nicht anklickbar sind. Im IE 8 lassen sich umbrochene URLs wie

http://www.heise.de/newsticker/Umfrage-
unter-Webarbeitern-im-deutschsprachigen-
Raum--/meldung/101383

komplett markieren und in die Adresszeile kopieren; IE entfernt die Zeilenumbrüche und fügt die Adresse als Ganzes ein.

Einen guten Eindruck hinterlässt das neue Zoom-Verhalten, das sich deutlich von dem seines Vorgängers abhebt. Der IE 7 zoomt noch recht unflexibel. Er betrachtet das Ergebnis des Rendering-Prozesses wie ein gedrucktes Blatt Papier und vergrößert oder verkleinert es als Ganzes: nicht nur die Schriften, sondern die gesamte Website inklusive aller Abstände, Größenangaben und Grafiken. Gerade bei flexiblen, seitenbreiten Layouts führt dieses Verhalten schnell zu Schwierigkeiten; denn das im Grunde flexible Layout wird wie ein fixes Layout behandelt, was schon in der ersten Vergrößerungsstufe zu horizontalen Rollbalken führt.

IE 8 hingegen verfügt über ein adaptives Zoomverhalten, eine Mischung aus Skalierung und Zoom. Anders als im IE 7 berechnet er die Seitenelemente beim Verkleinern oder Vergrößern neu und ordnet sie dementsprechend an. Breiten- und Höhenangaben in absoluten Einheiten oder solchen, die eine Abhängigkeit zum Gerät (beispielsweise *px*) oder zur Schrift (wie *ex* oder *em*) ausdrücken, skaliert der Browser; ein Zoom auf 200 % vergrößert 100 px auf 200 px und 5 mm auf 10 mm. Angaben, die sich auf die Umgebung beziehen, beispielsweise in % oder der Wert *auto*, werden nicht skaliert; was in der Standardgröße 50 % der Anzeigefläche ausmacht, bleibt

auch bei einem Zoom von 200 % nur 50 % der Anzeigefläche breit.

Zu den weiteren Neuerungen gehören die Wiederherstellung offener Tabs nach einem Absturz des Browsers, der in HTML 5 spezifizierte Speichermechanismus DOM Storage, ein verbesserter Phishing-Filter, integrierte Sicherheits- und Analysewerkzeuge sowie – laut Microsoft – zahlreiche Verbesserungen hinsichtlich Sicherheit, Stabilität und Geschwindigkeit.

Zwei Fliegen: Version Targeting

Ende Januar sorgte eine Ankündigung [a] im IEBlog für Aufregung und hitzige Diskussionen in der Blogosphäre. Nahezu alle in der deutschsprachigen und internationalen Szene bekannten Webworker meldeten sich zu Wort, um ihre Meinung über das von Wilson angekündigte Konzept des Version Targeting kund zu tun.

Er bezieht sich in seinem Beitrag auf einen Artikel im Onlinemagazin A List Apart (siehe [b]), der die drei Darstellungsmodi (siehe den Artikel über Doctype-Switching, [2]) des IE 8 vorstellt. Der Quirks-Modus stellt eine Webseite wie alte, inkompatible Internet Explorer dar; dabei entspricht der Quirks-Modus des IE 8 dem des IE 7. Daneben verfügt IE 8 über zwei standardkonforme Modi: einen herkömmlichen IE7-Standards-Modus, der dem des IE 7 mit all seinen Fehlern entspricht, und einen neuen (IE8-)Standards-Modus, der die komplett erneuerte Rendering Engine des IE 8 verwendet.

Über ein *meta*-Element können Webentwickler steuern, welchen der standardkonformen Modi sie auf ihre Website angewendet wissen wollen, beispielsweise den IE8-Standards-Modus:

```
<meta http-equiv="X-UA-Compatible"
  content="IE=8" />
```

Andere Browser als der IE lassen sich im Inhalt des *content*-Attributs ebenfalls aufführen. Über folgende Angabe gibt ein Webautor an, dass er die Webseite für IE 7, Firefox 3 und andere Browser in ihren jeweils aktuellen Versionen (Schlüsselwort *edge*) geschrieben hat:

```
<meta http-equiv="X-UA-Compatible"
  content="IE=7;FF=2;OtherUA=edge" />
```

Massiven Gegenwind aus der Webworker-Community verursachte der ursprüngliche Plan der IE-Entwickler, den neuen Browser standardmäßig im

IE7-Standards-Modus auszuliefern. Sie begründeten dieses Vorhaben mit denselben Argumenten, mit denen Microsoft 2001 das Doctype Switching eingeführt hatte: Der Internet Explorer soll lange Zeit und über mehrere Versionen hinweg abwärtskompatibel bleiben. Es soll kein Browser veröffentlicht werden, der zwar standardkonform arbeitet, aber gerade deshalb die existierenden, fehlerhaften Inhalte im Web nicht so darstellt, wie es sich Autoren dieser Inhalte wünschen. Mittlerweile hat Microsoft in die richtige Spur gefunden [c]: Schon in der ersten Beta-Version läuft der IE 8 mit dem IE8-Standards-Modus. Um den alten IE7-Standards-Modus zu veranlassen, können Webentwickler das oben genannte *meta*-Element einsetzen. Nutzer können in diesen Modus über die Schaltfläche „Emulate IE7“ wechseln (siehe Abb. unten), wofür sie den Browser in der aktuellen Beta-Version noch neu starten müssen.

Webstandards: Fortschritte und Versäumnisse

In Sachen Webstandards haben sich die IE-Entwickler viel vorgenommen: Sie haben sich zum Ziel gesetzt, den fertigen IE 8 mit vollständiger CSS-2.1-Unterstützung auszuliefern – ein respektables Ziel, vom dem die aktuelle Beta-Version jedoch noch weit entfernt ist. Um die CSS-Fähigkeiten des neuen Browsers zu überprüfen, erarbeiteten die IE-Entwickler über 700 Tests [d]. Diese und andere Testseiten [e], [f], [g] zeigen, dass noch viel Zeit vergehen dürfte, bis der IE so weit ist, dass Microsoft ihn veröffentlichen kann.

Eine wichtige Änderung: Das *has-Layout*-Konzept gibt es nicht mehr. Dabei handelt es sich um ein Konzept bis Version 7, das bestimmt, wie Elemente ihren Inhalt zeichnen und begrenzen, wie sie mit anderen Elementen interagieren und auf Benutzeraktionen reagieren. Elemente „haben“ Layout oder sie haben es nicht. Es gibt Elemente, die von vornherein Layout haben, bei anderen wird es durch die Vergabe von CSS-Eigenschaften ausgelöst, etwa bei absoluter Positionierung und den Eigenschaften *float*, *width* oder *height*. Das Layout-Konzept ist verantwortlich für viele *float*-Bugs, die IE 7 noch mit sich herumträgt. Mit der Eliminierung dieses Konzepts verschwinden im IE 8 viele dieser Fehler.

IE 8 unterstützt die Pseudoklasse *:focus* und die Pseudoelemente *:before* und *:after*, bei Letzteren allerdings nur die Schreibweise mit einem Doppelpunkt. Die in CSS 3 vorgesehene Schreibweise mit zwei Doppelpunkten (zum Beispiel *::before*), die helfen wird, Pseudoklassen und Pseudoelemente voneinander zu unterscheiden, erkennt IE 8 leider nicht.

Mit der Unterstützung der CSS-Eigenschaft *content* kommen nun auch IE-Nutzer in den Genuss der Kennzeichnung externer Links mittels folgender Regel, die Webentwickler so oder ähnlich seit Langem verwenden:

```
a[href^="http://"]::before,
a[href^="https://"]::before {
  content: "\2197\00A0";
}
```

Hinzugekommen ist die Unterstützung der Eigenschaft *outline* sowie einiger Eigenschaften für Print-Stylesheets (*page-break-inside*, *widows* und *orphans*). Die Unterstützung der Eigenschaft *display* schließt jetzt die Werte für Tabellen ein. Damit ist es möglich, Tabellen aus Nicht-Tabellen-Elementen zu erzeugen. Sinnvoll ist dies vor allem bei der Anwendung von CSS zur Formatierung von XML-Daten, die ein Browser anzeigen soll. Das im IE 7 noch teilweise fehlerhafte Konzept der zusammenfallenden Randabstände (margin collapsing) haben die Redmonder repariert.

Die IE-Entwickler haben das Tabellenmodell der getrennten Rahmen (separated border model) realisiert, das Rahmen nur für die Elemente *table*, *td* und *th* erlaubt, die mit einem kleinen Abstand voneinander dargestellt werden. In diesem Zusammenhang funktioniert auch die Anwendung der Eigenschaft *border-spacing*, über die Webentwickler den Abstand zwischen den Zellen angeben können. Bei der Eigenschaft *caption-side*, über die Webentwickler die Position von Tabellenüberschriften bestimmen können, interpretiert der IE 8 zwar neuerdings den Wert *bottom*, nicht jedoch die Werte *left* und *right*.

Für die Eigenschaft *list-style-type* interpretiert der IE 8 alle Werte aus CSS 2.1 und *upper-greek* aus CSS 3. Dies ist nicht das einzige, was die Entwickler aus CSS 3 übernommen haben. IE versteht die Eigenschaft *box-sizing* (allerdings in der Schreibweise *-ms-box-sizing*) zur Angabe eines alternativen CSS-Box-Modells.

Angesichts seines Beta-Status ist es nicht verwunderlich, dass IE 8 noch ziemlich viele Fehler aufweist, darunter solche, die der IE 7 nicht kennt. So werden beispielsweise die Eigenschaften *letter-spacing* und *word-spacing* sowie die Pseudoelemente *:first-line* und *:first-letter* nicht mehr interpretiert. Anker vererben ihren Cursor nicht, das heißt bei Markup wie

```
<a href="http://www.example.com">
<span>Link</span>
</a>
```

erscheint der Standard-Mauszeiger und nicht der Zeiger für die Verknüpfungsauswahl. Auch die Implementierung von CSS-Zählern (*counter-reset* und *counter-increment*) arbeitet noch nicht korrekt. Darüber hinaus gibt es zahlreiche weitere CSS-Fehler, die vielleicht schon zur nächsten Beta-Version, hoffentlich aber zur finalen Release des Browsers behoben sein sollten.

Leider nur wenig Verbesserung erfuhr die HTML-Unterstützung. Erwähnenswert ist nur die korrigierte Interpretation des *alt*-Attributs von Bildern. Dessen Inhalt erscheint nicht mehr als Tooltip, sondern kommt nur zur Anzeige, wenn das dazugehörige Bild nicht existiert. Korrekt verhält IE 8 sich allerdings nur bei einfachen *img*-Elementen. Bei grafischen Buttons (*input*-Elementen vom Typ *image*) und Image-Maps erscheint der *alt*-Inhalt gegebenenfalls weiterhin als Tooltip. Die Liste der weiteren Lücken, die die HTML-Unterstützung des IE 8 aufweist, ist nach wie vor lang: Die Attribute *cite* (für die Elemente *q*, *blockquote*, *ins* und *del*), *longdesc* (*img*) und *summary* (*table*) unterstützt die erste Beta-Version nicht; zumindest für *longdesc* ist Abhilfe zu erwarten. Das Element *q* zeigt ein Microsoft-Browser wohl niemals korrekt an, und ebenso wenig ist mit einer auf *link*-Elementen basierenden Navigation zu rechnen, auf die Webentwickler schon seit der Einführung von HTML 2.0 vor mehr als 12 Jahren warten. In der Beta hinzugekommen sind einige



An der URL ist erkennbar, dass es sich nicht um die Website einer Bank handelt – und rechts ist der Emulier-Button für IE 7 zu erkennen.

kleinere Fehler, beispielsweise ein verschobenes Rendering des *legend*-Elements. In kommenden Versionen dürften diese Fehler nicht mehr auftauchen.

Wie schon bei der Einführung des IE 7 verursacht die Tatsache Missstimmung, dass Microsoft die Chance ausgelassen hat, den Internet Explorer XHTML-fähig zu machen. Selbst der IE 8 wird nicht in der Lage sein, mit dem für XHTML-Dokumente vorgesehenen MIME-Typ *application/xhtml+xml* umzugehen. Wie bei seinen Vorgängern erscheint beim Aufruf einer auf diese Weise ausgelieferten Ressource ein Download-Dialog.

Browsertests mit Acid

Ein abschließender Blick auf die aktuellen Browsertests des Web Standards Projects (WaSP) hilft, den aktuellen Stand des Internet Explorer besser einzuordnen. Der Acid2-Test [h] wurde im April 2005 entwickelt und prüft hauptsächlich die CSS-Fähigkeiten. Mittlerweile bestehen alle wichtigen Browser den Test erfolgreich, darunter Safari, Konqueror, iCab, Opera und endlich aktuelle Beta-Versionen des Firefox 3. Während IE 7 an dem Test noch kläglich scheitert, zeigt IE 8 den gelben Smiley endlich in seiner vollen Pracht (siehe Artikelaufmacher, S. 52).

Der Acid3-Test [i] wurde im Februar 2008 veröffentlicht und konzentriert sich auf Tests interaktiver Anwendungen. DOM, ECMAscript, SVG, SMIL, und CSS 3 stehen im Fokus des Tests. Um ihn zu bestehen, muss ein Browser 100 Einzeltests erfolgreich absolvieren und das Ergebnis zudem korrekt darstellen können. Zur Veröffentlichung des Tests war dazu kein Browser in der Lage, mittlerweile schaffen es Beta-Versionen der Browser Safari 3.1 und Opera 9.5. Der IE 8 liegt weit zurück und schafft gerade mal 18 von 100 Tests.

Der Acid3-Test umfasst teilweise äußerst theoretische Szenarien, trotzdem schneiden alle modernen Browser besser ab als IE 8. Die Aussagekraft des Tests mag heute zwar noch bezweifelt werden, aber es bleibt das Gefühl zurück, dass Microsoft mit IE 8 seiner Konkurrenz wie damals mit IE 7 weiterhin einige Schritte hinterherhängt. (hb)

MICHAEL JENDRYSCHIK

ist Bereichsleiter Webentwicklung bei der itemis AG in Lünen. Er ist Buchautor und schreibt Fachartikel zu Web-Frontend-Themen.

Literatur

[1] Michael Jendryschik; Webdesign; Instandsetzung einer Ruine; Internet Explorer zwischen 6 und 7; *iX* 10/2006, S. 131

[2] Michael Jendryschik; Webdesign; Doctype-Switching: Wie Browser über die Darstellung von (X)HTML entscheiden; *iX* 3/2004, S. 136

iX-Link0805052

Onlinequellen

[a] Chris Wilson: Compatibility and IE 8	blogs.msdn.com/ie/archive/2008/01/21/compatibility-and-IE8.aspx
[b] Aaron Gustafson: Beyond DOCTYPE: Web Standards, Forward Compatibility, and IE 8	alistapart.com/articles/beyonddoctype
[c] Dean Hachamovitch: Microsoft's Interoperability Principles and IE8	blogs.msdn.com/ie/archive/2008/03/03/microsoft-s-interoperability-principles-and-ie8.aspx
[d] Windows Internet Explorer Testing Center	samples.msdn.microsoft.com/csstestpages/default.htm
[e] Gérard Talbot: 70 Bugs in MSIE 8 for Windows	www.gtalbot.org/BrowserBugsSection/MSIE8Bugs/
[f] Mark Wilton-Jones: Internet Explorer 8	www.howtocreate.co.uk/ie8.html
[g] Alan Gresley: Internet Explorer Bugs	css-class.com/test/bugs/ie/ie-bugs.htm
[h] Acid2 Browser Test	www.webstandards.org/action/acid2/
[i] Acid3 Browser Test	www.webstandards.org/action/acid3/
[j] CSS Improvements in Internet Explorer 8	msdn2.microsoft.com/en-us/library/cc304082(VS.85).aspx





Daten wiederherstellen mit Open-Source-Tools

Rausgefischt

Stefan Kelm

Ob gelöschte Dateien wiederherzustellen sind oder der Zugriff auf geschützte Festplattenbereiche gefragt ist – sogenannte Carving-Werkzeuge sind Ermittlern in vielerlei Hinsicht dienlich. Kein Wunder, dass zahlreiche Open-Source-Tools den kommerziellen Konkurrenz machen. Was taugen sie?

Immer häufiger hat man es im Rahmen forensischer Analysen mit gelöschten oder gar defekten Festplatten zu tun. Zu analysierende Systeme – insbesondere solche, die seit vielen Jahren in Verwendung sind – sind aber gerade in denjenigen Bereichen für den Forensiker interessant, auf die das Dateisystem jeglichen normalen Zugriff verweigert. Oft befinden sich gerade in den nicht (mehr) allozierten Speicherbereichen wertvolle Informationen.

Moderne Forensik-Tools, sogenannte File Carver, können hier bei der Rekonstruktion „ehemaliger“ Dateien helfen – dabei bietet auch die Open-Source-Welt interessante Alternativen. Bereits 2006 wurde daher eine systematische Vorgehensweise für derartige Rekonstruktionen vorgestellt [1]. Die damals erwähnten Tools hat der Autor einem Praxistest sowie einer Bewertung unterzogen.

Alle aktuellen Carving-Tools folgen zunächst einigen einfachen forensischen Grundsätzen: Den meisten Dateitypen liegt eine mehr oder weniger eindeutige Spezifikation des Dateiformats zugrunde und sie verfügen am Dateianfang – oft auch am Dateiende – über eine spezifische Byte-Folge, die eine eindeutige Identifikation des Dateityps ermöglicht. So starten zum Beispiel JPEG-Dateien immer mit *0xffd8ffe00010* und enden mit *0xffd9*. Auch das Unix-Kommando *file* verwendet diese Informationen [4].

Die Carving-Tools suchen nun nach diesen Byte-Folgen und kopieren („carven“) sämtliche Bytes, die dazwischenliegen, in eine neue Datei – fertig ist das rekonstruierte JPEG-Bild. Leider verfügen jedoch einige Dateitypen nicht über solche spezifischen Byte-Kombinationen am Dateiende.

Für diesen Fall (sowie für den Fall, dass die Datei auf der Festplatte fragmentiert ist) muss man dem Tool also eine maximale Anzahl zu carvender Bytes mitgeben und die extrahierte Datei anschließend manuell nachbearbeiten (Glück für die Forensikerin, dass es einige wenige Dateitypen gibt, die eine feste Dateigröße besitzen). Manchmal lässt sich die Länge einer Datei außerdem aus dem Datei-Header auslesen.

Ergänzende Handarbeit erforderlich

Die Kompilierung gestaltet sich bei allen Werkzeugen denkbar unkompliziert: In der Regel reicht ein einfaches *make*, unter Umständen gefolgt von einem *make install*, sofern das Tool gleich systemweit installiert werden soll. Je nach Unix-/Linux-Derivat ist ferner die eine oder andere Bibliothek (zum Beispiel *libcrypto*) nachzuinstallieren, bevor man carven kann. Bei den Open-Source-Tools ist anschließend die Anpassung einer ASCII-Konfigurationsdatei notwendig. In dieser Datei gibt man dem Tool genaue Instruktionen, welche Dateitypen es bis zu welcher Größe extrahieren soll.

Alle Tools erhielten dieselben forensischen Images: Die gängigen ([2] und [3]) frei zur Verfügung stehenden Testdateien enthalten auch Beschreibungen über den tatsächlichen Inhalt der Images, sodass man ziemlich schnell abschätzen kann, wie gut die Werkzeuge wirklich arbeiten. Bevor man jedoch loslegen kann, sollte man ausreichend Plattenplatz bereitstellen, da die Tools (mit Ausnahme von CarvFS) die identifizierten Dateien sofort extrahieren und dabei gelegentlich Dubletten erzeugen. Ein 50 MByte großes *dd*-Image kann daher durchaus deutlich mehr als 50 MByte an gecarvten Dateien erzeugen. Im Rahmen einer „sauberen“ forensischen Analyse muss man eine eigens dafür bestimmte Platte verwenden.

iX-TRACT

- Für die Wiederherstellung gelöschter Daten oder den Zugriff auf geschützte Speicherbereiche gibt es Open-Source-Werkzeuge, die es durchaus mit ihrer kommerziellen „Konkurrenz“ aufnehmen können.
- Zwar bieten sie keine grafische Oberfläche, in ihren Eigenschaften – Offenheit für neue Formate, Geschwindigkeit et cetera – stehen sie den kommerziellen Produkten aber nicht nach.
- Einen „Platzhirsch“ gibt es nicht – zumal ein guter Ermittler nicht zuletzt aufgrund der unterschiedlichen Funde je Werkzeug immer mehrere von ihnen einsetzt.

Foremost 1.5.3

Eines der ersten und bis heute meistverwendeten Tools ist das von der Air Force programmierte Foremost. Die aktuelle Version 1.5.3 lässt sich – ebenso wie die nachfolgend beschriebenen Werkzeuge – problemlos mit *gcc* übersetzen und sofort benutzen. Vor dem ersten Einsatz muss man jedoch die Konfiguration anpassen, die sich in der Datei *foremost.conf* befindet (Listing 1). In ihr sind alle diejenigen Dateitypen auszukommentieren, nach denen man suchen will.

Man sollte sich also vorher Gedanken darüber machen, ob man beispielsweise eher Multimediadaten oder aber Office-Dokumente rekonstruieren will: eine für forensische Analysen durchaus übliche Vorgehensweise, da man an dieser Stelle in der Regel bereits ausreichend Anhaltspunkte für zu suchende Dateiformate gewonnen hat. Im Zweifelsfall können natürlich auch sämtliche von Foremost unterstützende Dateitypen verwendet werden. In diesem Fall wird aber sicher eine Vielzahl von „unbrauchbaren“ Dateien erzeugt, die der Ermittler anschließend manuell sichten muss.

Nach dem Anlegen des Zielverzeichnisses (hier *carv-output*) kann das Tool gestartet werden:

```
foremost -i /Images/11-carve-fat.dd ↵
      -o ./carv-output -c ./foremost.conf
```

Im Ziel-Directory finden sich anschließend eine Reihe von Unterverzeichnissen (zum Beispiel *jpg*), in denen

```
Eingabeaufforderung
Image file pass 1/2.
Read 10485760 bytes from image file.
usbkey.dd:   8.0% |**                              |   10.0 MB    00:00 ETA
A doc header was found at : 700416
Memory reallocation performed, total header storage = 101
A doc footer was found at : 700416
Memory reallocation performed, total footer storage = 101
A doc header was found at : 700416
Memory reallocation performed, total header storage = 101
Read 10485760 bytes from image file.
usbkey.dd:  16.0% |*****                           |   20.0 MB    00:01 ETA
A doc header was found at : 15132672
A doc footer was found at : 15132672
A doc header was found at : 15132672
Read 10485760 bytes from image file.
usbkey.dd:  24.0% |********                        |   30.0 MB    00:03 ETA
Read 10485760 bytes from image file.
usbkey.dd:  32.0% |**********                      |   40.0 MB    00:02 ETA
A doc header was found at : 38848512
A doc footer was found at : 38848512
A doc header was found at : 38848512
Read 10485760 bytes from image file.
usbkey.dd:  39.9% |*************                   |   50.0 MB    00:02 ETA
Read 10485760 bytes from image file.
usbkey.dd:  47.9% |***************                 |   60.0 MB    00:02 ETA
```

Scalpel, das aus einer Neuprogrammierung des Tools Foremost hervorging, bringt eine vorkompilierte Windows-Version mit (Abb. 1).

Listing 1

```
#
# Foremost configuration file (EXTRACT)
#-----------------------------------------------------------------
# GRAPHICS FILES
#-----------------------------------------------------------------
#
# GIF and JPG files (very common)
#  (NOTE THESE FORMATS HAVE BUILTIN EXTRACTION FUNCTION)
   gif   y   155000000   \x47\x49\x46\x38\x37\x61   \x00\x3b
   gif   y   155000000   \x47\x49\x46\x38\x39\x61   \x00\x00\x3b
   jpg   y   20000000    \xff\xd8\xff\xe0\x00\x10   \xff\xd9
   jpg   y   20000000    \xff\xd8\xff\xe1           \xff\xd9
   jpg   y   20000000    \xff\xd8                   \xff\xd9
#
# BMP
#  (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
   bmp   y   100000      BM??\x00\x00\x00
#-----------------------------------------------------------------
# ANIMATION FILES
#-----------------------------------------------------------------
#
# MPEG Video
   mpg   y   4000000     mpg     eof
   mpg   y   20000000    \x00\x00\x01\xba   \x00\x00\x01\xb9
   mpg   y   20000000    \x00\x00\x01\xb3   \x00\x00\x01\xb7
#
# Macromedia Flash
#  fws   y   4000000     FWS
#
#-----------------------------------------------------------------
# MICROSOFT OFFICE
#-----------------------------------------------------------------
#
# Word documents
#  (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
   doc   y   12500000    \xd0\xcf\x11\xe0\xa1\xb1
#
# Outlook files
   pst   y   400000000   \x21\x42\x4e\xa5\x6f\xb5\xa6
   ost   y   400000000   \x21\x42\x44\x4e
#
#-----------------------------------------------------------------
# HTML  (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
#-----------------------------------------------------------------
#
   htm   n   50000       <html             </html>
#
#-----------------------------------------------------------------
# ADOBE PDF  (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNC-
TION)
#-----------------------------------------------------------------
#
   pdf   y   5000000     %PDF-   %EOF
#-----------------------------------------------------------------
# SOUND FILES
#-----------------------------------------------------------------
#  wav   y   200000      RIFF????WAVE
#
#  wma   y   8000000     \x30\x26\xB2\x75   \x00\x00\x00\xFF
#
#  wma   y   8000000     \x30\x26\xB2\x75   \x52\x9A\x12\x46
#
   mp3   y   8000000     \xFF\xFB??\x44\x00\x00
   mp3   y   8000000     \x57\x41\x56\45    \x00\x00\xFF\
   mp3   y   8000000     \xFF\xFB\xD0\      \xD1\x35\x51\xCC\
   mp3   y   8000000     \x49\x44\x33\
   mp3   y   8000000     \x4C\x41\x4D\x45\
#-----------------------------------------------------------------
# MISCELLANEOUS
#-----------------------------------------------------------------
#  (NOTE THIS FORMAT HAS BUILTIN EXTRACTION FUNCTION)
#  zip   y   10000000    PK\x03\x04         \x3c\xac
#
#  java  y   1000000     \xca\xfe\xba\xbe
```

In der Konfigurationsdatei muss man vor Beginn alle Dateitypen, nach denen man suchen will, auskommentieren.

Foremost die extrahierten Dateien ablegt. Der Ermittler kann sie dann sichten und bewerten.



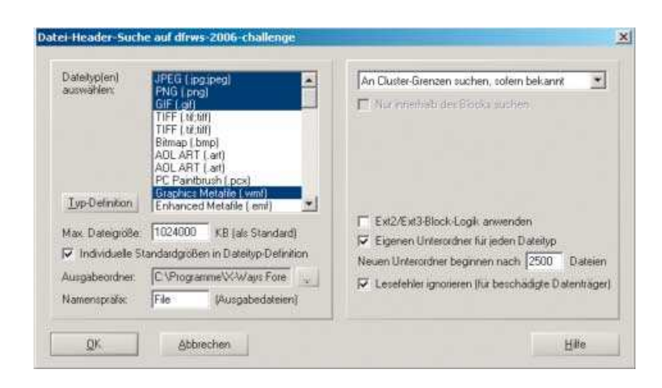
Scalpel 1.60

Bei Scalpel handelt es sich um ein ähnliches Werkzeug, das auch in der Benutzung kaum Unterschiede zeigt. Das ist nicht weiter verwunderlich, entstand es doch aus der kompletten Neuprogrammierung von Foremost, die insbesondere die Performanz erhöhen sollte. Die Installation des Tools ist daher nahezu identisch, selbst die Konfigurationsdatei *scalpel.conf* kommt einem sofort bekannt vor (tatsächlich kann Scalpel auch die Datei *foremost.conf* lesen). Eine vorkompilierte Windows-Version wird ebenfalls mitgeliefert (Abb. 1).

Man startet das Tool mit

```
scalpel -p -c ./scalpel.conf ↵
                /Images/11-carve-fat.dd
```

Ergebnisse werden in das Verzeichnis *scalpel-output* geschrieben, allerdings nur, wenn es leer ist. Befinden sich dort noch Dateien, bricht das Tool mit einer Warnung ab, um nicht versehentlich ehemals extrahierte Dateien zu überschreiben. Die Option *–p* erlaubt es der Forensikerin, eine Art Probedurchlauf (preview) durchzuführen, bei der das Tool nicht extrahiert, sondern nur die gefundenen Treffer in der Datei *audit.txt* auflistet (Listing 2).



Kommerzielle Werkzeuge, hier X-Ways Forensics, benutzen dieselben Techniken wie Open-Source-Tools, jedoch in der Regel unter einer grafischen Benutzeroberfläche „versteckt“ (Abb. 2).

Listing 2

```
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Image file pass 1/2.
/Images/dfrws-2006-challenge.raw:  21.0% |   |   10.0 MB   00:00 ETA
/Images/dfrws-2006-challenge.raw:  41.9% |*  |   20.0 MB   00:00 ETA
/Images/dfrws-2006-challenge.raw:  62.9% |*  |   30.0 MB   00:00 ETA
/Images/dfrws-2006-challenge.raw:  83.9% |** |   40.0 MB   00:00 ETA
/Images/dfrws-2006-challenge.raw: 100.0% |***|   47.7 MB   00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 0 files
gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" --> 0 files
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 19 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 0 files
bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 1 files
tif with header "\x49\x49\x2a\x00" and footer "" --> 0 files
tif with header "\x4d\x4d\x00\x2a" and footer "" --> 2 files
mov with header "\x3f\x3f\x3f\x3f\x6d\x6f\x6f\x76" and footer "" --> 0 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer
"\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --> 6 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 6 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 0 files
wav with header "\x52\x49\x46\x46\x3f\x3f\x3f\x3f\x57\x41\x56\x45" and footer ""
--> 0 files
zip with header "\x50\x4b\x03\x04" and footer "\x3c\xac" --> 13 files
Carving files from image.
Image file pass 2/2.
/Images/dfrws-2006-challenge.raw:  21.0% |   |   10.0 MB   00:00 ETA
/Images/dfrws-2006-challenge.raw:  41.9% |*  |   20.0 MB   00:00 ETA
/Images/dfrws-2006-challenge.raw:  62.9% |*  |   30.0 MB   00:00 ETA
/Images/dfrws-2006-challenge.raw:  83.9% |** |   40.0 MB   00:00 ETA
/Images/dfrws-2006-challenge.raw: 100.0% |***|   47.7 MB   00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 47, elapsed = 3 seconds.
```



CarvFS

Noch einen Schritt weiter gehen Tools, die das sogenannte „In Place Carving“ beherrschen. CarvFS und vergleichbare Werkzeuge etwa extrahieren die Dateien nicht, die sie in einem Image finden, sondern legen symbolische Links an, die direkt auf die entsprechenden Bytes dort verweisen. Diese Technik benötigt also ungleich weniger Speicherplatz während der forensischen Analyse, was sich gerade bei großen Festplatten bemerkbar machen kann.

Bei CarvFS handelt es sich um ein auf dem Kernelmodul FUSE basierendes virtuelles Dateisystem, in dem die zu suchenden Dateien wie gewohnt verwendet werden können. Der Befehl

```
carvfs /mnt/carvfs raw ↵
                /Images/11-carve-fat.dd
```

führt dazu, dass eine bestimmte Dateistruktur unterhalb von */mnt/carvfs/* angelegt wird, die wie folgt aussehen kann:

```
total 128179
d--x--x--x 3 root root       0 Jan  1 ↵
                         1970 CarvFS
-r--r--r-- 1 root root 131252224 Jan  1 ↵
                         1970 CarvFS.crv
-rw-rw-rw- 1 root root    2545 Jan  1 ↵
                         1970 README
-rw------- 1 root root      95 Jan  1 ↵
                         1970 ocfa.missing
```

Auf dieser Dateistruktur kann anschließend mit den schon bekannten Tools (aber auch anderen forensischen Suiten wie „The Sleuthkit“ alias TSK) gecarvt werden:

```
scalpel -p -c ./scalpel.conf /mnt/carvfs/ ↵
    0000000000000000000000000000000000/ ↵
                              CarvFS.crv
```

Scalpel kam hier im Preview-Modus zum Einsatz, der nur eine einfache Textdatei erzeugt. CarvFS erlaubt jetzt mit dem mitgelieferten Skript *scalpelcp*, die Ergebnisse dieser Textdatei zu interpretieren und die Suchtreffer als symbolische Links zu den betreffenden Stellen im virtuellen Dateisystem anzulegen.

Der Befehl

```
scalpelcp ./scalpel-output/ /mnt/carvfs/ ↵
    0000000000000000000000000000000000/ ↵
                                 CarvFS/
```

führt beispielsweise zu folgenden symbolischen Links auf gefundene Bilder:

```
lrwxrwxrwx 1 root root   69 Jul 18 15:40 ↵
  00000677.gif -> /mnt/carvfs/00000000000 ↵
      00000000000000000000000/CarvFS/ ↵
                      64525824:3430.crv
lrwxrwxrwx 1 root root   69 Jul 18 15:40 ↵
00000678.gif -> /mnt/carvfs/00000000000000 ↵
      00000000000000000000/CarvFS/ ↵
                      65545728:2802.crv
lrwxrwxrwx 1 root root   66 Jul 18 15:40 ↵
        00000679.jpg -> /mnt/carvfs/ ↵
    0000000000000000000000000000000000/ ↵
                  CarvFS/34304:4310.crv
lrwxrwxrwx 1 root root   66 Jul 18 15:40 ↵
00000680.jpg -> /mnt/carvfs/0000000000000 ↵
      000000000000000000000/CarvFS/ ↵
                         43008:2344.crv
```

43008:2344.crv bedeutet, dass beim Offset 43008 eine 2344 Bytes große Datei beginnt. Durch die symbolischen Links kann man folglich eine ganze Menge an Plattenplatz einsparen.

Damit es nicht frühere Funde überschreibt, enthält Scalpel eine Funktion für einen Probedurchlauf, bei dem es nur die Treffer anzeigt und nicht gleich die gefundenen Daten extrahiert.

X-Ways Forensics

Last but not least soll an dieser Stelle exemplarisch auch auf eines der zahlreichen kommerziellen Forensikwerkzeuge eingegangen werden. Alle diese Tools beherrschen selbstverständlich

auch unterschiedliche Carving-Mechanismen, verpacken diese Funktion aber wie erwartet in mehr oder weniger intuitiv zu bedienende GUIs.

X-Ways Forensics bietet beispielsweise in der aktuellen Version 14.8 mit den Menüpunkten „Dateien retten nach Typ“ sowie „Datei-Header-Signatursuche“ gleich zwei unterschiedlich mächtige Verfahren an (Abb. 2). Die darunterliegende Technik ist jedoch vergleichbar mit den oben erwähnten Tools.

Die grafische Oberfläche erlaubt ferner die komplette forensische „Bearbeitung“ der gecarvten Dateien innerhalb eines Programms, zum Beispiel auch einen in der Praxis recht nützlichen Vorschaumodus (Abb. 3).

Im laufenden Betrieb

Da die getesteten Werkzeuge sich nur in Details voneinander unterscheiden, kann ihre Bewertung an dieser Stelle gemeinsam erfolgen.

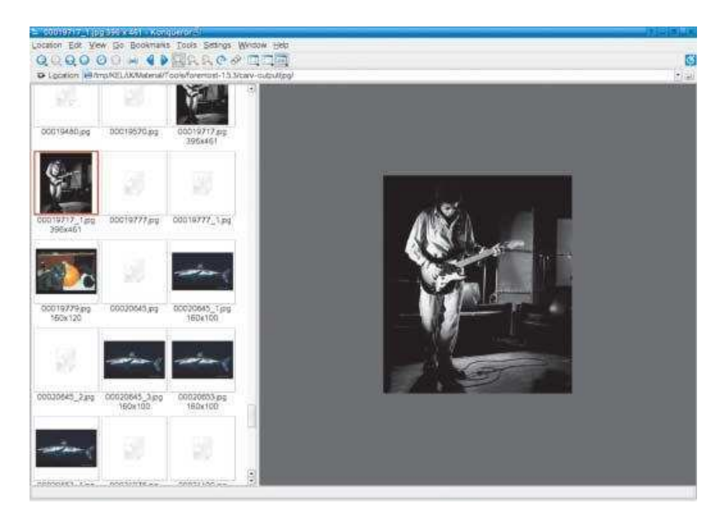
Sämtliche hier beschriebenen Tools sind sehr schnell. Auf einem normalen Arbeitsplatzrechner sind alle in der Lage, 50 bis 150 MByte große Images in wenigen Sekunden zu durchforsten. Dabei ist es wichtig, stets die aktuellen Versionen einzusetzen, da die Entwickler oft noch an der Performanz der Werkzeuge feilen.



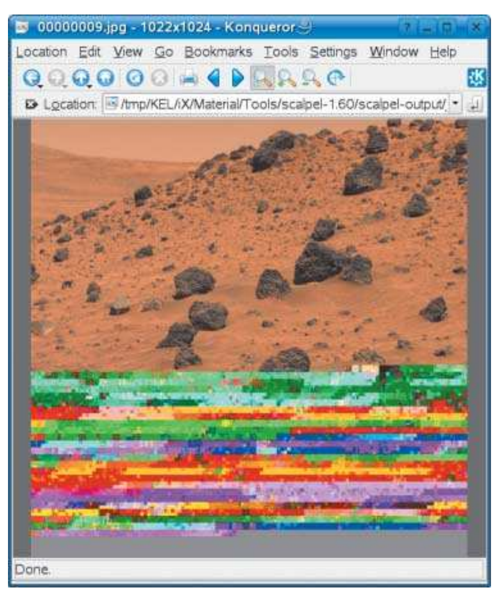
Die nützliche Vorschaufunktion des kommerziellen Tools erlaubt eine schnelle Einordnung der gefundenen Dateien (Abb. 3).

Mit Ausnahme von CarvFS benötigen alle Werkzeuge unter Umständen extrem viel Speicherplatz, um die rekonstruierten Dateien ablegen zu können. Hier sollte also nicht an Festplattenplatz gegeizt werden. Dies liegt auch und insbesondere daran, dass alle Tools üblicherweise viele Dubletten sowie „False Positives“ liefern, die man anschließend manuell herausfiltern muss (Abb. 4).

Da das Dateiende etlicher Dateitypen nicht definiert ist oder von den Tools aufgrund von Fragmentierung nicht erkannt wurde, sind die rekonstruierten Dateien oft viel größer, als es die Originale waren. Will man also im Rahmen einer forensischen Analyse etwa ein rekonstruiertes GIF-Bild mit einem anderen Bild vergleichen, kann man mit einem üblicherweise durchgeführten Prüfsummenvergleich (MD5, SHA1 et cetera) nichts erreichen. Die Dateien kann man sich dennoch meist mit den normalen Viewern problemlos anschauen (Abb. 5).



Dubletten und falsch-positive Funde kosten immens viel Speicherplatz und müssen überdies manuell aussortiert werden (Abb. 4).



Selbst wenn ein rekonstruiertes Bild defekt ist, lässt es sich mit Viewern noch anschauen – per Prüfsummen-vergleich identifizieren kann man es allerdings nicht (Abb. 5).

Original-Dateinamen können die Tools nicht rekonstruieren (man kann diese jedoch gegebenenfalls durch andere forensische Methoden wiederherstellen), sondern die Bilder heißen beispielsweise *00000677.gif*. Auch das ist jedoch kein forensisches Problem.

Die Standardkonfiguration aller Tools ist bereits sehr umfangreich, dennoch muss man mit den Konfigurationen je nach zu analysierendem Image ein wenig „spielen“, um zu brauchbaren Resultaten zu kommen. Einige Dateiformate sollten bewusst ausgeblendet werden (aber welche?) und auch die maximale Dateigröße ist bestenfalls als Empfehlung zu sehen. Andererseits sind die Tools flexibel genug, selbst neue oder eigene (proprietäre) Dateiformate schnell definieren zu können. Orientieren kann man sich hier etwa an Quellen wie www.wotsit.org.

In der Praxis rücken die beschriebenen Einschränkungen jedoch je nach zu lösender Aufgabe in den Hintergrund, wenn es beispielsweise nur darum geht, „eindeutige“ (z. B. kinderpornografische) Inhalte zu finden.

Die Erfolgsquote der einzelnen Tools hängt auch stark von der richtigen Konfiguration ab (etwa in Bezug auf die maximale Dateigröße). Daher wurde an dieser Stelle auf die Nennung expliziter Zahlen bewusst verzichtet und lediglich eine Einschätzung vorgenommen. In der Standardkonfiguration arbeiten alle Tools zuverlässig und unterstützen den forensischen Prozess erheblich. Wer an konkreten Zahlen interessiert ist, sei auf die Arbeit von Bas Kloet [7] verwiesen. Dort vergleicht der Autor ein selbst entwickeltes Tool (Revit) mit Foremost und Co.

Fazit

File Carving wird für den IT-Forensiker immer wichtiger. Glücklicherweise gibt es eine Reihe vielversprechender Tools, die bei der Wiederherstellung von Dateien helfen. Dabei muss man nicht unbedingt tief in den Geldbeutel greifen, um gut funktionierende Software zu bekommen. Wie für alle anderen forensischen Tools gelten aber auch hier die folgenden Grundsätze: Einerseits müssen die Ergebnisse der Tools in der Regel manuell nachbearbeitet sowie insbesondere korrekt interpretiert werden, andererseits unterscheiden sich die Ergebnisse im Detail so stark voneinander, dass man sich nie auf ein einzelnes Tool verlassen sollte. Es soll daher an dieser Stelle keine Empfehlung für ein bestimmtes Tool geben – keines arbeitet perfekt.

An ihre virtuellen Grenzen kommen alle verfügbaren Tools mehr oder weniger schnell, wenn die zu untersuchende Festplatte sehr stark fragmentiert oder schlicht viel zu groß ist. Dafür gibt es im Forschungsumfeld bereits heute vielversprechende Ansätze – zum Beispiel basierend auf Entropie-Untersuchungen –, die die Tool-Sammlung der Forensiker sicher zukünftig erweitern werden [5, 6]. (ur)

STEFAN KELM

ist Mitarbeiter der Secorvo Security Consulting GmbH und liebt Carving – sowohl auf der Skipiste als auch auf Festplatten.

Literatur

[1] Oliver Tennert; Dateisystemforensik; In letzter Minute; Post-mortem-Analyse von Filesystemen unter Linux; *iX* 3/2006, S. 38

[2] Digital Forensics Tool Testing Images; dftt.sourceforge.net

[3] DFRWS 2006 Forensics Challenge Overview; dfrws.org/2006/challenge

[4] Brian Carrier; File System Forensic Analysis; Addison-Wesley; 2005

[5] Michael Cohen; Advanced Carving techniques; 2007 sandbox.dfrws.org/2007/cohen/Advanced_Carving.pdf

[6] Andreas Schuster; File Carving – Grundlagen und neue Techniken; 2007

[7] Bas Kloet; Measuring and Improving the Quality of File Carving Methods; 2007; www.uitwisselplatform.nl/frs/download.php/461/thesis.pdf

Onlinequellen

Foremost	foremost.sourceforge.net
Scalpel	www.digitalforensicssolutions.com/Scalpel
CarvFS	sourceforge.net/projects/ocfa

iX-Wertung

Foremost

⊕ sehr schnell
⊕ flexibel für neue Formate
⊖ benötigt viel Speicherplatz

Scalpel

⊕ sehr schnell
⊕ flexibel für neue Formate
⊖ benötigt viel Speicherplatz

ScarvFS

⊕ sehr schnell
⊕ flexibel für neue Formate
⊕ benötigt wenig Speicherplatz



Drupal 6: Neue APIs und mehr Komfort

Gemeinsam ans Web

Markus Franz

Drupal ist ein Web-Content-Management-System, das sich besonders bei Web-2.0-Communities großer Beliebtheit erfreut. Vor Kurzem haben die Entwickler die Major Release 6.0 und gleich danach Version 6.1 freigegeben.

Will man eine Website aufbauen, kommt man in vielen Fällen nicht an einem professionellen Content-Management-System vorbei. Ein Großteil der auf dem Markt verfügbaren Open-Source-Produkte (siehe [1]) basiert auf PHP – für Drupal gilt das ebenfalls. Es ist ein etabliertes System, das prominente Kunden einsetzen: Warner Brothers, Amnesty International ebenso wie Sony BMG, Forbes und die Harvard University.

Drupal stellt keine unerfüllbaren Forderungen an das Zielsystem: Das CMS arbeitet zuverlässig mit Apache ab 1.3 und Microsofts IIS ab 6.0, mit denen man PHP 5.x verwendet – andere Server mit PHP-Unterstützung funktionieren theoretisch ebenfalls. Empfohlen sind hierfür die üblichen Standardmodule für XML sowie GDLib und Imagemagick. Als Datenbank dienen MySQL 4.3 beziehungsweise PostgreSQL 7.4 oder aktuellere Editionen. Drupal arbeitet weiterhin nur optimal mit Zugriff auf *cron*, damit regelmäßig wiederkehrende Aufgaben bearbeitet werden können. Diesem Artikel liegen Apache 2.2, PHP 5.2 sowie MySQL 5.0 auf einem Dell Inspiron 1525 unter Ubuntu Linux 7.10 zugrunde.

Drupal zeichnet sich vor allem durch Ansätze von sozialer Software aus, wodurch es sich gut für den Aufbau einer Community, Weblogs oder eines sozialen Netzes eignet – kurzum für viele Projekte im Web 2.0. Nicht erst seit Version 6.0 enthält Drupal zahlreiche Module, die folgende Kernfunktionen ermöglichen:
– Erstellen und Bearbeiten von Seiten und Artikeln in Kategorien,
– Anlegen von Blogs und zugehörige Kommentarverwaltung,
– Zusammenfassen von webbasierten Büchern und Forum,
– Workflow-Management und Rechteverwaltung für Benutzer.

Interessant sind besonders die (XML-) APIs, mit denen man die Inhalte externen Anwendungen bereitstellen kann. Über Zusatzmodule lässt sich Drupal komfortabel beispielsweise mit einem WYSIWYG-Editor ergänzen. Am 13. Februar haben die Entwickler nun die Major Release der Version 6.0 veröffentlicht, die vor allem dem hohen Anspruch an Stabilität, Erweiterbarkeit, Internationalisierung und Bedienung Rechnung tragen soll. Eine Bugfix-Version 6.1 folgte noch im Februar.

Drupal kommt über die Projektwebsite www.drupal.org als erfreulich kleiner Download daher: Das Archiv ist nur knapp 1 MByte groß. Das mag für den Download zwar unerheblich erscheinen, wirkt beim Upload auf den eigenen Webserver aber angenehm. Dennoch hat sich Drupal enorm vergrößert: Die letzte Version der Serie 5 war noch knapp 740 KByte groß, Version 4.7 schlug mit unter 500 KByte zu Buche. Im Vergleich zu anderen CMS ist Drupal aber immer noch angenehm schlank.

iX-TRACT

- Drupal 6.x erlaubt die Aufteilung unterschiedlicher Aufgaben auf mehrere Abteilungen.
- Neben verbesserter Sprachunterstützung sind die Highlights das neue Setup und der Update-Manager sowie die Content-Aktionen.
- Die Integration von OpenID und Drag&Drop-Verwaltung vervollständigen das positive Bild.

Installer mit mehreren Profilen

Für den Download hat man die Qual der Wahl: Neben der Standardausgabe stehen verschiedene weitere Distributionen bereit, die „Installation Profiles“ heißen. Die passen je nach Zielgruppe das CMS in Design, Standardseiten und Einstellungen an. Zwar ist dieses Feature schon

mit Version 5 hinzugekommen, ab Drupal 6 arbeiten die Profiles aber mit dem neuen Installer besser zusammen. So kann man beispielsweise für Konferenzen speziell angepasste Webseiten einfach aufsetzen.

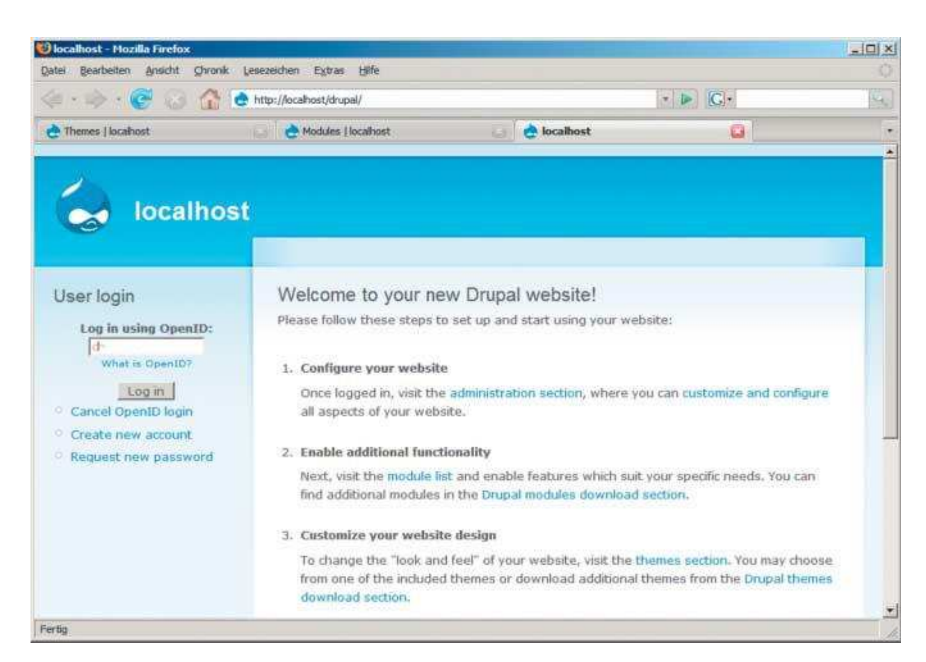
Der neue Installer ist ein komplett überarbeitetes Highlight der Version 6. Er liefert ein von lokaler Software gewohntes Interface mit einer Anzeige der Punkte am linken Rand: Sobald einer erledigt ist, wird dieser mit einem Haken markiert. Insgesamt durchläuft der Installationsprozess folgende Schritte: Im ersten Anlauf wählt man aus, ob Drupal in englischer Sprache oder einer anderen zu installieren ist. Zusätzlich verfügbare Sprachen werden direkt in den Installer importiert, sodass man diese direkt auswählen kann – angenehm ist, dass der Assistent gleich in der gewählten Sprache weitermacht.

Bei der Systemumgebung hat sich kaum etwas zu Version 5 geändert. Man sollte aber von Anfang an auf PHP 5.2 setzen, da dies eine zwingende Voraussetzung für die nächsten Versionen sein soll. Nachdem man die Zugangsdaten für die Datenbank angegeben hat (MySQL oder PostgreSQL), ist die Installation mit der Konfiguration der Website (Titel, URL et cetera) abgeschlossen.

Nach der Installation prüft Drupal automatisch, ob das Modul „Clean URLs“ (URL Rewriting) aktiviert werden kann – in diesem Fall muss man nicht mehr manuell die Einstellungen in der Administration kontrollieren und aktivieren. Das Files-Verzeichnis eigenhändig einzurichten, ist nicht mehr erforderlich – sofern die entsprechenden Rechte gesetzt sind, legt der Installationsassistent dieses automatisch an.

An der blauen Oberfläche

Die fertige Installation von Drupal 6 kommt im gleichen blauen Gewand daher wie die Vorversion. Beeindruckend fällt das neue Drag & Drop in der Administration auf: An vielen Stellen kann man einfach durch Ziehen und Ablegen die Inhalte verändern. Unter anderem kann man die Menübäume der Website ebenso platzieren wie die Inhalte einer Seite. So lässt sich beispielsweise der Seitentitel beliebig verschieben – faszinierend für ein webbasiertes CMS. Unter Safari zeigten sich aber immer wieder kleine Fehler beim Verschieben, die bei anderen Browsern nicht auftreten sollten. Drag & Drop lässt sich auch im Forum, auf hochgeladenen Dateien oder Feldern in Benutzerprofilen nutzen.



Identitätsmanagement über Plattform- und Anwendungsgrenzen hinweg: Benutzer können sich mit OpenID bei Drupal 6 anmelden (Abb. 1).

Außerdem hat Drupal die Internationalisierung wie angesprochen verbessert: Nicht nur im Installer, sondern auch im laufenden Betrieb werden neue Sprachen automatisch erkannt und aktiviert, ebenso wie neue Module oder Designthemen. Zusätzlich gibt es das Modul „Localization Client“, mit dem über eine Ajax-basierte Oberfläche die gerade betrachtete Seite übersetzt werden kann. Gleichzeitig ermöglicht dieses Modul den Import von Übersetzungen aus Drupal 5 und erleichtert so die Migration.

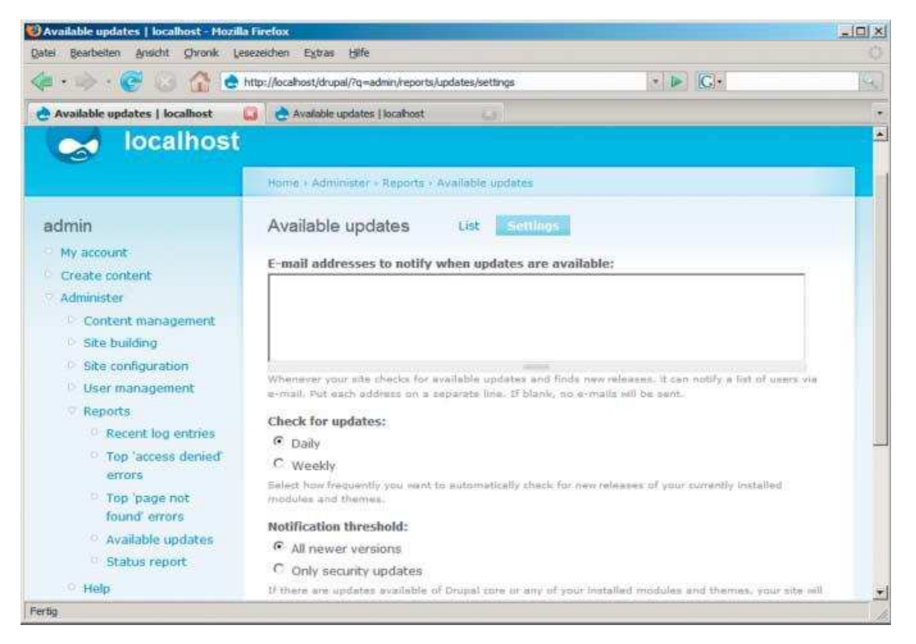
Die bedeutendste Änderung in Version 6 ist aber die Unterstützung von OpenID – ein System zum Identitätsmanagement über Plattform- und Anwendungsgrenzen hinweg: Jeder kann einen OpenID-Server betreiben und sich anmelden. Dabei hat der Nutzer den Vorteil, sich nicht Hunderte Kombinationen von Name und Kennwort merken zu müssen: Über die einheitliche Online-Identität kann jeder so an Drupal teilnehmen. Für den Aufbau einer Community kann dies ein entscheidender Vorteil gegenüber der Konkurrenz sein, da es die Hemmschwelle zur Mitarbeit senkt – allerdings ist OpenID in Deutschland noch kaum verbreitet.

Hat man sich mit dem neuen CMS ein wenig angefreundet, fällt ein weiteres Leistungsmerkmal auf: die Content-Aktionen. Über den Actions-Dialog kann man genau festlegen, ob etwa eine E-Mail bei einem neuen Post versendet werden soll oder der Benutzer einen Hinweis enthält. Diese Aktionen lassen sich über ein Dropdown-Menü auf Posts, Benutzer und Kommentare anwenden. So hat man außer der bisher etablierten Rechteverwaltung und dem Workflow-Support eine weitere Option, Projekte effizient zu koordinieren und komplexe Zusammenhänge zwischen Benutzern und Seiteninhalten abzubilden.

Verwaltung von Inhalt und Vorlagen

Für Webdesigner bietet Drupal 6 Spannendes: reine CSS-Designs, die ohne eine einzige Zeile HTML- oder PHP-Code auskommen. Sie basieren auf einer einzigen *.info*-Datei, in der man Abhängigkeiten definieren kann. Mit Drupal lassen sich Entwicklung, Administration und Themen in verschiedenen Abteilungen bearbeiten, die komplett unabhängig arbeiten können.

Gleichzeitig existiert ein Modul, das speziell für Themenentwickler gedacht ist. Damit lassen sich nicht nur Abhängigkeiten, sondern außerdem Seitenbereiche sowie Funktionen und Klassen anzeigen. Diese Zusatzinformationen machen das System zu einer interessanten Option für Webdesigner, die kommerzielle Designs entwerfen. Möchte man nur einfache Änderungen am bestehenden Thema vornehmen, ist das mit der neuen Release erheblich einfacher: Jeder noch so kleine Abschnitt



Nur für den Admin oder für eine Gruppe: Der automatische Updater prüft regelmäßig auf Neuerungen (Abb. 2).

kann über eine reine HTML-Datei verändert werden – man muss daher nicht über PHP-Kenntnisse verfügen. Schon aus den Namen der Dateien für das Template (wie *forum-icon.tpl.php*, *forum-list.tpl.php*) lässt sich der Sinn des Elements schnell erschließen.

Darüber hinaus enthält Drupal jetzt eine aktualisierte jQuery-Javascript-Bibliothek, die das CMS intensiv nutzt und die sich für eigene Entwicklungen direkt einsetzen lässt. Überhaupt taucht in der neuen Version an allen Ecken und Enden ein Javascript-basiertes Interface auf: Auf der einen Seite erhöht das den Komfort, lässt andererseits Browser mit mangelhaftem Support für Javascript/Ajax scheitern.

Benachrichtigung des Admin

Sensible Bereiche beim Betrieb eines Content-Management-Systems sind Geschwindigkeit und Sicherheit. Beide Aspekte lassen kaum Kompromisse zu und machen es den Entwicklern in der Open-Source-Szene nicht immer einfach: Insbesondere die prominenten (Unternehmens-)Kunden haben hohe Erwartungen an ein CMS. Das Drupal-Team versucht, diese zunächst mit einem neuen Update-Manager zu erfüllen: Als erstes Web-CMS benachrichtigt Drupal den Administrator, sobald Sicherheitsupdates verfügbar sind. Über Updates für Module und Themen wird man ebenfalls informiert.

Gibt man beim Anlegen eines neuen Benutzerkontos ein Kennwort ein, sorgt die neue Release ebenfalls für mehr Sicherheit: Sie zeigt gleich die Stärke des Passworts an und warnt den Anwender bei zu schwachen Eingaben. Neben einigen Änderungen im Detail, die zur Sicherheit beitragen, haben die Entwickler ein Security Team gebildet. Dieses koordiniert Sicherheitsaspekte des CMS sowie Meldungen von Anwendern und organisiert Security Fixes. Das Team hat außerdem dafür gesorgt, dass die angewachsenen Kernmodule in mehrere kleine aufgeteilt wurden, die sich besser überwachen lassen.

Drupals Geschwindigkeit haben die Entwickler auf verschiedenen Ebenen signifikant optimiert. Das System läuft nun hinter einem Reverse Proxy (beispielsweise Squid). Gleichzeitig werden Dateien jetzt nicht mehr einzelnen Posts, sondern wieder Benutzern zugeordnet, was die Handhabung erleichtert. Neue Funktionen prüfen Format und Größe, was sich ebenfalls positiv auf die Geschwindigkeit auswirkt.

Zu guter Letzt beinhaltet Drupal 6 zwei neue APIs:
– Schema-API: Mit dieser Schnittstelle kann man auf die Datenbank hinter dem CMS zugreifen und Tabellen verwalten. Es bietet besseren Support für andere Datenbanken als MySQL. (Man darf gespannt sein, wann der geplante Oracle-Support endlich stabil ist.)
– Batch-API: Schnittstelle für zeitaufwendige Prozesse, die im Hintergrund bearbeitet werden können. Es zeigt den Fortschritt der Aktionen an.

Zu den dargestellten Neuerungen kommen einige Veränderungen im Detail. In jedem Fall sollte man bei einem Update auf die neue Major Release vorsichtig sein: Es empfiehlt sich, mit einer sauberen neuen Installation zu starten und anschließend die Inhalte und Designs sowie Module schrittweise zu migrieren. Viele Kernmodule sind in ihrer Struktur verändert, und die Entwickler haben konzeptionell viel erneuert – nur mit einer sauberen Installation kann man sich eine stabile Umgebung einrichten.

Fazit

Mit OpenID, den Verbesserungen bei Sicherheit und Stabilität sowie dem erweiterten Komfort bei Benutzerverwaltung und Design durch Drag & Drop schließt Drupal nicht nur zu anderen Content-Management-Systemen auf. Es übertrifft diese teilweise an Qualität und Erweiterbarkeit sowie bei der Internationalisierung. Und es setzt sich damit an die Spitze für Communities. Im Unternehmensumfeld bleibt es spannend, ob die PHP-basierte Plattform sich hier weiter durchsetzen kann. (hb)

MARKUS FRANZ

ist Mitgründer und CTO der BF Blogform Search GmbH, Berlin. Er studiert Wirtschaftsinformatik an der Friedrich-Schiller-Universität in Jena.

Literatur

[1] Denny Carl; Web Content Management I; Webwelten; Für Groß und Klein: Fünf CMS auf PHP-Basis; *iX* 12/2007, S. 54

iX-Wertung

⊕ Integration von OpenID zur Benutzeranmeldung

⊕ neuer Update-Manager für Aktualisierungen

⊕ Administration verwendet Ajax im Browser.

⊖ alte Module und Plug-ins laufen nicht mehr

⊖ Drupal setzt Zugriff auf *cron* voraus.



Main Pyrus: Archivierung auf Open-Source-Basis

Akten unter Strom

Jochen Kokemüller



Jedes Unternehmen hat mit Unmengen an Dokumenten zu tun, die es zum großen Teil revisionssicher und über Jahre aufbewahren muss. Programme für das Dokumentenmanagement sind teuer, Open-Source-Lösungen rar. Main Pyrus DMS ist eine der wenigen Ausnahmen.

Ab einer bestimmten Betriebsgröße wächst die Verwaltung überproportional und damit auch die Menge der zu verwaltenden Schriftstücke. Hinzu gesellen sich die von den Fachabteilungen erstellten Rechnungen, Bestellungen, technischen Zeichnungen und so weiter. Vieles davon unterliegt rechtlichen Rahmenbedingungen, Rechnungen muss eine Firma beispielsweise zehn Jahre aufheben, Geschäftsbriefe darf sie schon nach sechs Jahren vernichten. Um die Aktenberge sicher zu lagern, ist die Firma oft gezwungen, zusätzliche Räumlichkeiten anzumieten. Hier steckt natürlich erhebliches Rationalisierungspotenzial durch digitale Archivierung.

Erfahrungen des Fraunhofer IAO zeigen, dass die Lizenzen für ein archivbetontes Dokumentenmanagementsystem (DMS) ohne Workflow-Komponenten 200 bis 400 Euro pro Arbeitsplatz kosten. Hinzu kommt das Anpassen an die jeweilige Umgebung, das rund die Hälfte bis das Doppelte der Lizenzkosten ausmacht. Für ein mittelständisches Unternehmen ist hier die Schmerzgrenze schnell erreicht.

Als Alternative zu den kommerziellen DMS findet man bisher nur wenige Open-Source-Produkte, darunter jedoch einige Perlen. Drei stechen besonders heraus: Alfresco, Nuxeo und Main Pyrus DMS. Bei allen stehen Unternehmen im Hintergrund, die sich um die Weiterentwicklung kümmern. Allerdings sind die beiden erstgenannten nicht im deutschen Markt aktiv, sie konzentrieren sich auf Großbritannien beziehungsweise Frankreich. Main Pyrus DMS existiert seit 2003, hauptverantwortlich für diese Software zeichnet die Main IT in Kelkheim. Sie achtet darauf, dass nur stabile Versionen auf den Markt kommen. Neben der deutschen Version gibt es englische, rumänische und ungarische Varianten.

Ein verbreitetes DMS-Konzept sind Dokumentenklassen wie *Rechnung* und *Bestellung*. Attribute, etwa *Rechnungs-Nr*. oder *Datum*, beschreiben die Klassen näher. Main Pyrus verfügt über umfangreiche Möglichkeiten, solche Klassen und Attribute anzulegen und zu konfigurieren. Das System lässt sich so einrichten, dass beispielsweise eine Rechnungsnummer zwingend ist, das Format der Steuernummer vorgegeben und die Auswahl von Artikelnummern aus einer Liste erfolgen muss.

Dokumente in der Klassengesellschaft

Ein Dokument gehört in Main Pyrus immer zu einer Klasse. Es darf mehreren Klassen zugeordnet sein, etwa wenn es gleichzeitig als Lieferschein und Rechnung fungiert oder wenn sich dadurch verschiedene Sichten erstellen lassen, wie öffentliche und interne Informationen zu Ausschreibungen.

Die Suche nach bestimmten Dokumenten ist über alle Dokumentenklassen möglich, zum Beispiel via Klassenattribut *Kunden-Nr*. Steht die Kundennummer allerdings nicht auf der Bestellung, findet man auch nichts. Hier hilft ein mächtiges Konzept, nämlich das der Projekte. Sie orientieren sich an Mappen, die mehrere Dokumente enthalten (etwa Kundenakten). Sie werden, wie die Klassen, mit Attributen beschrieben, beispielsweise wieder mit der Kundennummer. In diesem Fall wäre es unerheblich, wenn diese auf dem einzelnen Dokument fehlt.

Papierdokumente gehören in der Regel nur zu einer Mappe. Viele DMS realisieren diese Gruppierung durch Pfade wie im Dateisystem. Doch bei Pfaden verhält es sich wie bei den Mappen: Ein Dokument liegt nur an einer Stelle. In Main Pyrus hingegen darf ein Dokument zu beliebig vielen Projekten gehören, Pfade existieren hier nicht.

Der Administrator kann Benutzer und Gruppen anlegen. Eine Besonderheit ist, dass Gruppen wiederum zu Gruppen gehören dürfen. Dadurch lassen sich sowohl Gruppen als auch Rollen abbilden. Die Rollen *Mitarbeiter Service* und *Leitung Service* werden als Gruppen definiert, wobei Letztere möglicherweise nur ein Mitglied hat. Sie können wiederum zur Gruppe *Service*

gehören, die Tiefe dieser Hierarchien ist nicht limitiert.

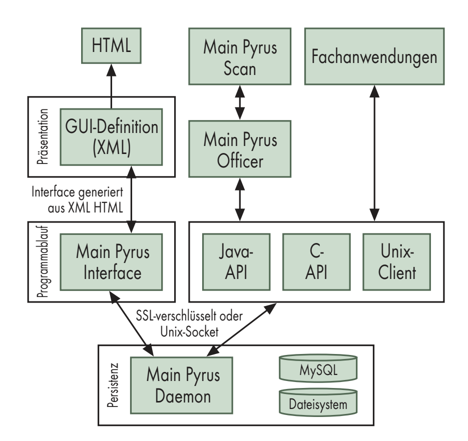
Dokumente, Klassen, Projekte und Projekttypen lassen sich mit Rechten ausstatten. Für den Zugriff auf ein Dokument ist allerdings nur das Recht an ihm selbst entscheidend, die Rechte an Klassen und Projekttypen ermöglichen lediglich die Suche. Zusätzlich regeln die Rechte, wer bestimmte Projekte oder Dokumente anlegen darf.

Komplizierte Verwaltung der Rechte

Es gibt positive, neutrale und negative Rechte, Letztere sind eine Besonderheit in Main Pyrus. Dahinter steht die Überlegung, dass sich Rechte über komplizierte Vererbungsbeziehungen durch Gruppenzugehörigkeiten und Vertretungen übertragen lassen. In der Konsequenz ist es nicht möglich, einzelnen Benutzern den Zugriff auf Dokumente dediziert zu verbieten. Genau dieses leistet das negative Recht.

Beim Dokumentenaufruf überschreibt ein gefundenes negatives Recht alle positiven Rechte und verhindert somit den Zugriff. Doch auch hier gilt: keine Regel ohne Ausnahme. Vertretungsbeziehungen (beispielsweise Urlaubsvertretungen) geben zwar die positiven, aber nicht die negativen Rechte weiter. Diese Ausnahme ist notwendig, denn ansonsten könnte der Zugriff auf ein Dokument versperrt sein, weil der Vertretene es nicht sehen darf.

Dieses komplizierte Rechtesystem hat Nachteile. Es ist undenkbar, dass eine Suchanfrage es schafft, alle Beziehungen dynamisch aufzulösen. Die Entwickler entschlossen sich daher, alle



Alle Systemkomponenten dürfen grundsätzlich auf separaten Rechnern laufen, was eine gute Skalierung verspricht (Abb. 1).

Rechtebeziehungen in zyklischen Intervallen auf simple Tabelleneinträge herunterzubrechen. Einfache Rechteänderungen übernimmt das System sofort. Komplizierte Aktionen, wie das Anlegen eines neuen Benutzers oder einer neuen Vertretung, wirken erst nach einem *flush privileges*, den das System voreingestellt jede Nacht ausführt.

Leider bietet das DMS keine Funktion für den Import von Benutzerprofilen. Da dieser Vorgang meist nur einmal (bei Inbetriebnahme des Produktes) notwendig ist, kann dies ein Dienstleister im Rahmen der übrigen Datenmigration erledigen.

Wer Dokumente aus einer Fachanwendung automatisiert in Main Pyrus exportieren will, muss sie mit Metadaten beschreiben und diese in einer XML-Datei ablegen. Hier stehen dann alle Informationen zu Klassen, Benutzern, Gruppen und Projekten. Main Pyrus lässt sich so einstellen, dass es automatisch Projekte anlegt und die übertragenen Dateien hier über eine Vorgangsnummer richtig einsortiert.

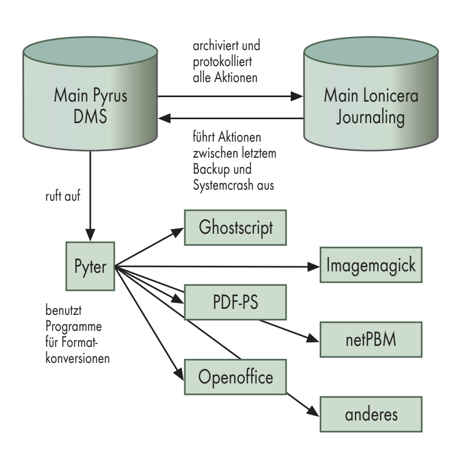
Viele Pfade führen ins System

Für die Übergabe der XML-Datei existieren mehrere Wege. Einerseits über die nativen Java- und C-APIs oder per Kommandozeile am Linux-Client. Die Kommunikation mit dem Main-Pyrus-Server wird SSL-verschlüsselt (OpenSSL), die Authentifizierung über SSL-Zertifikate abgewickelt. Alternativ (bei einer lokalen Verbindung) erfolgt die Authentifizierung aus Geschwindigkeitsgründen via Unix-Sockets. Das DMS skaliert gut in großen Umgebungen, denn Systemkomponenten wie Daemon, Interface, Datenbank, Dateisystem, Officer und Scan-Client können auf verschiedenen Maschinen laufen (Abbildung 1). Ein Betrieb im Cluster ist möglich.

Der genannte Server (*Main Pyrus Daemon*) bildet das Backend. Seine Aufgaben sind das Einspielen neuer Dokumente, das Zugriffsmanagement sowie die Wartung des Rechtesystems. Für Letztere benutzt er eine eigene, an SQL angelehnte Domain Specific Language (DSL). Wenn der Administrator etwa das Rechtesystem erneuern will, gibt er auf der Kommandozeile ein:

```
$>pyrus -u admin -p passwort -q "flush privileges"
```

Sind die Dateien aus dem Fremdsystem in Main Pyrus angekommen, wandelt

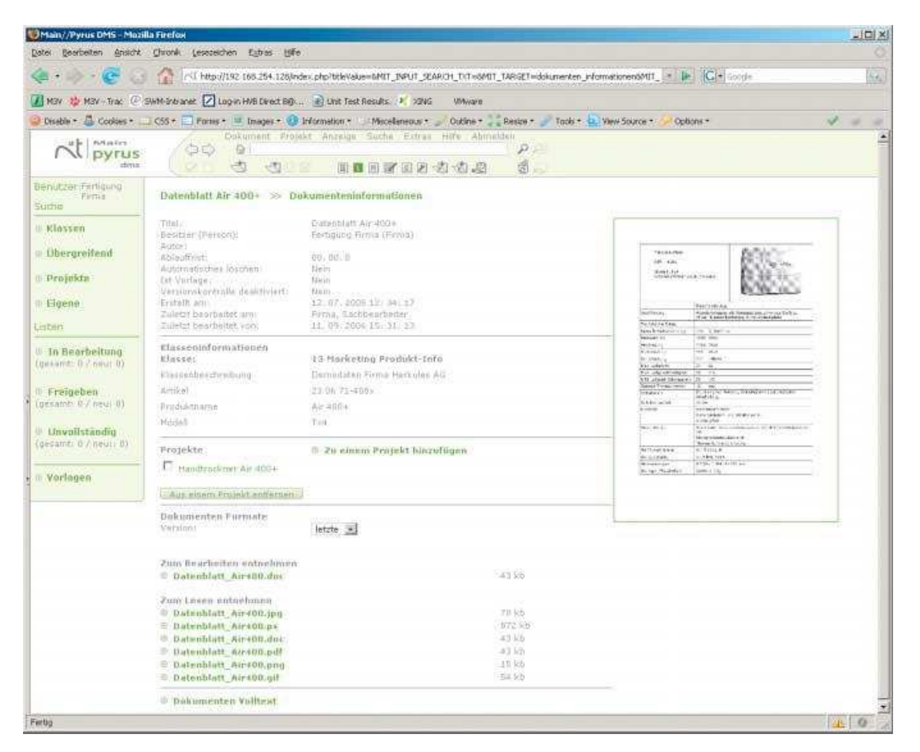


Das Web-Interface bietet den populärsten Systemzugang. Hier die Ansicht eines Dokuments mit allen seinen konvertierten Formaten (Abb. 2).

das DMS sie in die gewünschten Formate um. Hintergrund: Ein Unternehmen muss wie anfangs erwähnt auf viele digitale Unterlagen auch nach einer langen Zeitspanne noch zugreifen können. Die Fachanwendung, aus der die Dokumente stammen, hat dann möglicherweise schon lange das Zeitliche gesegnet. In PDF/A oder TIFF konvertierte Dokumente sind wesentlich zukunftssicherer als irgendwelche proprietären Formate.

Die Formatwandlung erledigt das Konvertierungs-Framework Pyter. In einer Konfigurationsdatei legt der Anwender seine unterschiedlichen Ein- und Ausgangsformate sowie die Konvertierungsprogramme fest, die er einsetzen will, beispielsweise die netPBM-Suite oder Imagemagick. Im zweiten Schritt erzeugt das Framework eine Liste der Verarbeitungsketten, die alle möglichen Pfade zwischen Eingabeformat und Ausgabeformat enthält. Dann sortiert das Framework die Pfade nach den Kosten, also nach dem kürzesten Weg. Am günstigsten wäre eine Ein-zu-eins-Konvertierung ohne Umweg über ein drittes Programm oder Format. Pyter beginnt mit dem ersten Pfad und versucht die Konvertierung. Klappt die nicht, nimmt es den nächsten Pfad und so weiter. Dieser Ablauf garantiert eine recht sichere Formatwandlung in automatisierten Prozessen, da man die jeweils besten Programme dafür einsetzen kann und diese Arbeit nicht bei Main Pyrus hängenbleibt.

Im Regelfall arbeitet der Benutzer mit den Dokumenten über das Web-Interface (Abbildung 2). Es setzt sich zusammen aus einer PHP-Anwendung, die die Programmabläufe steuert, sowie den XML-Dateien für die Seitenbeschreibung. Programmcode und Präsentation



Für Journaling und Formatkonvertierung setzt Main Pyrus die separaten Komponenten Lonicera und Pyter ein (Abb. 3).

sind also klar getrennt. Die Oberfläche ist aus einer Art angereichertem HTML aufgebaut, vergleichbar mit JSP. Die XML-Dateien lassen sich leicht anpassen, ohne dass man den Programmcode ändern oder gar verstehen muss. Die Ausgabe des Dokumententitels als HTML-Überschrift 1 könnte beispielsweise so aussehen: *<h1><mit:doc_title/></h1>*. Eine leider unüberschaubare Liste aller vorhandenen XML-Tags liegt unter: *./src/tokens/xml_tokens.php*. Zwar lässt sich die Oberfläche darüber an eigene Vorstellungen anpassen, dieses Unterfangen erfordert allerdings sehr großen Aufwand.

Alle angefertigten Webseiten liegen in *./main-it*. Wenn man dieses Verzeichnis kopiert und die Konfigurationsdatei *./conf.php* entsprechend modifiziert, kann Main Pyrus kundenspezifische Ausprägungen der Seiten generieren. Dies ist insbesondere dann interessant, wenn es für mehrere Mandanten geschehen soll, beispielsweise im gehosteten Betrieb.

Einen weiteren Baustein stellt der Journaling-Server Main Lonicera dar, der jede Änderung an den Dokumenten mitschreibt. Alle Aktionen ab einem bestimmten Zeitpunkt kann der Administrator (etwa nach einem Plattencrash) neu starten (Abbildung 3). Bedienen muss er den Server per Kommandozeile, ein Web-Interface wäre natürlich wünschenswert.

Es existieren mehrere Möglichkeiten, ein Dokument im DMS abzulegen. Einerseits kann der Input aus den angebundenen Fremdsystemen erfolgen, andererseits per direkter Übergabe an den Unix-Client. Für die letztgenannte Option bietet Main Pyrus Übertragungsfunktionen via E-Mail oder FTP. All diese Wege eignen sich insbesondere für automatisierte Verfahren.

Für die manuelle Dokumentenablage gibt es ebenfalls zwei Varianten. Einerseits über die Weboberfläche (Menüpunkt: *neues Dokument hinzufügen* und andererseits per Java-Anwendung *Main Pyrus Officer*. Die Dokumente kann man manuell auswählen, über ein Openoffice-Plug-in übernehmen oder via *Main Pyrus Scan* scannen. Letztere Anwendung beherrscht das Einlesen von Stapeln, das nachträgliche Sortieren der Seiten, sowie das Gruppieren zu unterschiedlichen Projekten. Leider lassen sich MS-Office-Programme bisher nicht einbinden.

Fazit

Main Pyrus ist ein ausgewachsenes DMS mit Archivierungsschwerpunkt. Es bietet keine Workflow-Komponenten, beispielsweise für einen automatisierten Zeichnungsprozess, dafür Mandantenfähigkeit und gute Skalierungsfähigkeiten. Bemerkenswert sind die hohe Sicherheit vor Datenverlust, die das Modul Main Lonicera schafft, die flexible Ablagestruktur sowie die Anpassungsfähigkeit an individuelle Bedürfnisse.

Diese Eigenschaften überzeugten das Fraunhofer IAO davon, das DMS in einem vom Bundesministerium für Wirtschaft und Technologie geförderten Projekt einzusetzen. Ein mittelständischer Maschinenbauer arbeitet ebenfalls damit. Weitere Unternehmen planen die Migration.

Für mittelständische Firmen stellt das Open-Source-Produkt Main Pyrus eine ernstzunehmende Alternative zur lizenzkostenpflichtigen Konkurrenz dar. Allerdings darf man nicht erwarten, gänzlich kostenlos davonzukommen. Einen IT-Dienstleister benötigt man für Wartung und Betrieb schon. Allerdings ist man bei der Wahl frei und nicht an einen Hersteller gebunden. Beispielsweise bieten Gonicus oder Netcon Support an. Dass Main Pyrus unter der GPL steht, verspricht Investitions- und Zukunftssicherheit. (jd)

JOCHEN KOKEMÜLLER

ist wissenschaftlicher Mitarbeiter am Fraunhofer Institut für Arbeitswirtschaft und Organisation (IAO). Seine Schwerpunkte liegen in den Bereichen DMS, SOA und mobile Anwendungen.

Onlinequellen

Main-Pyrus-Homepage
www.mainpyrus.org

Main-Pyrus-Downloads
sourceforge.net/projects/mainpyrus/

Main IT
www.main-it.de

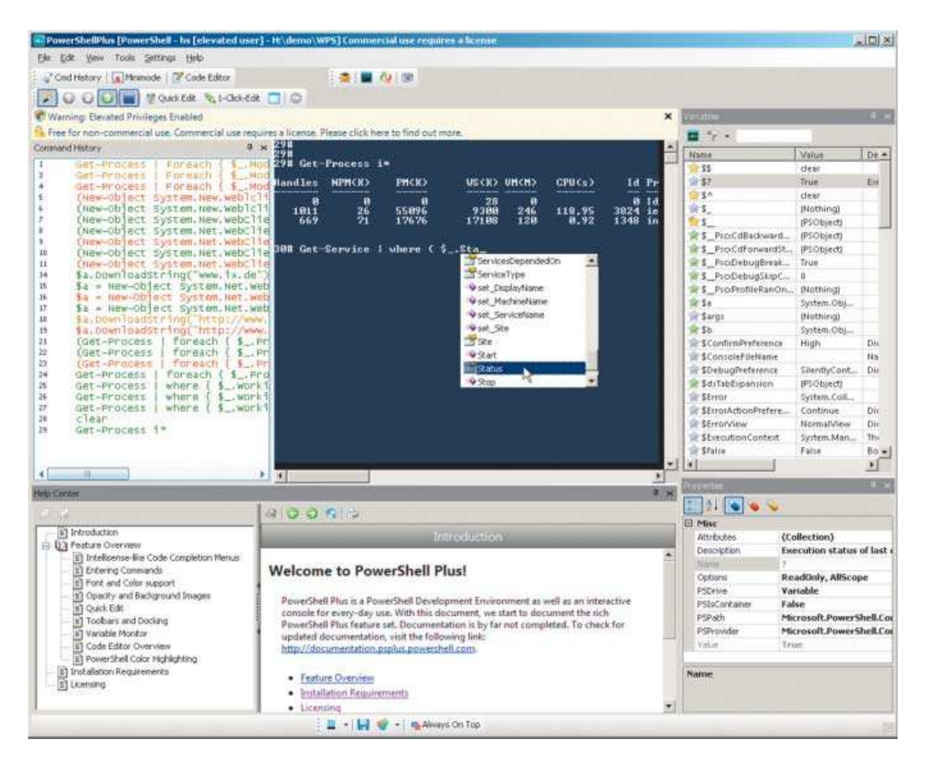
Journaling-Modul Main Lonicera
sourceforge.net/projects/mainlonicera/

Konvertierungs-Framework Pyter
sourceforge.net/projects/pyter/

iX-Wertung

⊕ flexible Ablagestruktur
⊕ hohe Datensicherheit
⊕ skaliert gut
⊕ Investitionssicherheit

⊖ keine Workflow-Komponenten
⊖ keine MS-Office-Integration



PowerShellPlus: Eine IDE für Microsofts neue Shell

Muschel verpackt

Holger Schwichtenberg

Die wegen ihrer Leistungsfähigkeit viel gepriesene PowerShell bietet bisher nur eine unkomfortable Benutzeroberfläche. Microsoft hat es bisher nicht geschafft, der Shell ein angemessenes GUI zu verpassen. Diese Lücke schließt nun das Third-Party-Tool PowerShellPlus.

Beim ersten Start der Windows PowerShell ist sicher mancher Administrator enttäuscht, denn er sieht nur ein schwarz-weißes Kommandozeilenfenster, wie man es seit Jahren von der *cmd* her kennt. Aus den ursprünglichen Redmonder Ankündigungen, die Konsole mit IntelliSense auszustatten, ist bis heute nichts geworden.

Man kann zwar Commandlet-Namen und -Parameter mit der Tabulator-Taste vervollständigen, dennoch bietet die Shell prinzipiell kaum mehr Komfort als die alte Muschel. Von der Unterstützung eines Visual Studio ist die Konsole weit entfernt. Für die Bearbeitung von Skripten (*.ps1*-Dateien) bietet Microsoft keine andere Lösung als *notepad* an.

Die PowerShellPlus hingegen zeigt sich bereits beim ersten Start mit umfangreicher Menü- und Symbolleiste sowie mehreren Fenstern (s. Abbildung oben). Vorweg ist zu bemerken, dass diese IDE intern auf der Version 1.0 der Original-Shell aufsetzt und alle Befehle beziehungsweise Skripte, die man hier erstellt, vollständig kompatibel zu den Befehlen der von Microsoft ausgelieferten Konsole sind.

IDE bringt mehr Komfort

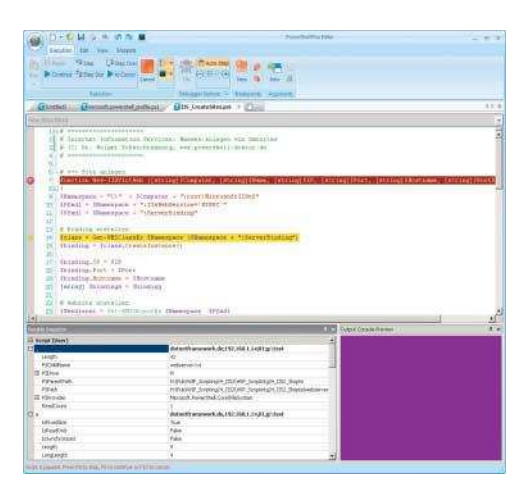
PowerShellPlus vereinfacht die Erfassung und das Testen von Befehlen. Man benötigt das Tool aber nur auf dem System, an dem der Administrator interaktiv arbeitet. Zur Laufzeit (zum Beispiel bei Anmeldeskripten) reicht die normale PowerShell aus. Da alle klassischen Kommandozeilenbefehle der *cmd* in der neuen Shell und damit in der IDE ausführbar sind, können auch Administratoren, die noch mit der *cmd* arbeiten, von der Plus-Konsole profitieren.

Bei einigen der Darstellungsoptionen, die die PowerShellPlus bietet, kann man sich nur fragen, wieso diese in der Redmonder Version fehlen. In diese Kategorie gehören sicherlich die stufenlose Vergrößerung des Fensters und die Unterstützung für Kopier- und Einfügeaktionen mit Strg + C und Strg + V. Vollen Einfluss auf die Schriftarten hat man, wenn als Unterbau Vista oder der 2008-Server werkelt.

Der wesentliche Vorteil liegt in der Eingabeunterstützung bei der Erfassung von Befehlen. Die IDE bietet hier Vorschlagmenüs im Stil der IntelliSense vom Visual Studio. Sie hilft bei der Eingabe von Commandlet-Namen und -Parametern sowie bei Variablennamen, Pfadangaben und direkten .Net-Anwendungen. Besonders eindrucksvoll ist die Eingabeunterstützung bei der Nutzung von .Net-Klassen über das Commandlet *New-Object* und dem anschließenden Zugriff auf Klassenmitglieder. Auch für Klassen der Windows Management Instrumentation (WMI) gibt es Vorschläge, wenn man eine Eingabe nach *Get-WmiObject* mit den typischen Klassenpräfixen *WIN32_* oder *CIM_* beginnt.

PowerShell-Editor von Microsoft

Im Zuge von Version 2.0 der PowerShell will Microsoft auch einen Skripteditor liefern. Aktuell ist die „Graphical PowerShell“ noch grausam rudimentär: Sie bietet nur Syntaxhervorhebung und eine Ausführungsumgebung für Befehle und Skripte. Eingabehilfen durch Tabulatorvervollständigung und IntelliSense im Stil von Visual Studio sind aber geplant. Immerhin kann man schon jetzt über mehrere Registerkarten verschiedene sogenannte PowerShell Runspaces gleichzeitig betreiben. Die Vorabversion bekommt man unter www.microsoft.com/downloads/details.aspx?FamilyID=60deac2b-975b-41e6-9fa0c2fd6aa6bc89&displaylang=en. Sie war bei Redaktionsschluss aber noch auf dem Stand „November 2007“.



In Aktion: der Skriptdebugger in der PowerShellPlus

Bei mehrstufigen Befehlen fragt PowerShellPlus, ob sie denn den ersten Teil des Befehls ausführen darf, um die korrekten Vorschläge anzeigen zu können. Dies sollte der Nutzer nur bei idempotenten Befehlen bejahen. In einer Whitelist kann der Systemverwalter Befehle aufnehmen, die man zu Analysezwecken gefahrlos ausführen kann. In die Blacklist hingegen gehören Befehle, die niemals zu diesem Zweck eingesetzt werden dürfen (zum Beispiel *Remove-Item*). Leider zeigt PowerShellPlus in manchen Situationen trotz Nachfrage entweder keine Optionen oder nicht die korrekte Liste der Möglichkeiten an. Helfen kann hier die Aufteilung des Befehls auf mehrere Zeilen durch Verwendung von Variablen.

Das seitliche Fenster „Variables" zeigt den Inhalt aller aktuell verfügbaren PowerShell-Variablen an. Dazu gehören neben den selbsterstellten Variablen die eingebauten wie *$_*, *$_args*, *$home* und *$error*. Das unter diesem Fenster liegende „Properties"-Fenster zeigt Details zu einer ausgewählten Variable an. Wenn die Variable ein komplexes Objekt ist, sieht man die Mitglieder. Wenn die Variable eine Objektmenge enthält, kann man zwischen den einzelnen Elementen auswählen und deren Mitglieder betrachten; das ist aber noch wenig intuitiv zu bedienen.

Die verschiedenen Teilfenster kann der Anwender wie in Visual Studio verschieben und andocken. So auch das optional einblendbare „Command History", das die Liste der letzten Befehle zeigt. Alle Befehle kann man in einer Textdatei protokollieren lassen oder in die Zwischenablage legen.

Ein weiteres Standbein der PowerShellPlus ist der im optischen Stil von Office 2007 gehaltene Editor für Skriptdateien. Das sind einfache Textdateien mit der Dateikennung *.ps1*. Grundsätzlich könnte jeder Texteditor zum Einsatz kommen, nur erwarten professionelle Benutzer heutzutage sprachspezifische Unterstützung und farbliche Syntaxhervorhebung der Sprachschlüsselwörter.

Mit Skripteditor und Debugger

Neben Farbhervorhebung bei der Eingabe bietet der Skripteditor den gleichen Komfort wie die dazugehörige Konsole. Zudem können Skripte automatisch gemäß der Blockebenen eingerückt werden. Aus dem Visual Studio hat man die Code-Regionen übernommen, mit denen man Blöcke zusammenklappen kann; das dient der Übersichtlichkeit bei umfangreicheren Skripten.

Der Hersteller liefert den Editor mit zahlreichen vorgefertigten Code-Fragmenten („Code Snippets"), die der Nutzer in eigene Skripte einfügen kann. Auch das Erstellen eigener Fragmente ist möglich. Den Editor kann man zusätzlich für C#-, VB.Net-, HTML- und XML-Dateien verwenden – einschließlich IntelliSense. Für XML-Dateien kann man eine Schemadatei angeben. Direkt aus dem Editor heraus kann der Administrator sein Skript starten, das dann im Kontext der Plus-Konsole läuft.

Ein Highlight im Editor ist der Debugger, der ein Skript an frei definierbaren Punkten anhalten und dann Befehl für Befehl durchlaufen kann (s. Abbildung). Wenn das Skript im Zustand „Pause" ist, lässt sich der Zustand der im Skript verwendeten Variablen im Editor oder „Variables"-Fenster der Konsole betrachten. Alternativ kann man interaktiv an der Konsole in das Skript eingreifen.

Der Debugging-Prozess hat im Editor nicht nur seine Funktion zur Fehlersuche, sondern darüber hinaus für die IntelliSense. Da ein Commandlet nicht deklariert, welche Objekte es in die Pipeline gibt, und die Ausgabe eines Commandlets kontextabhängig sein kann, weiß der Editor nicht, welche Möglichkeiten zur Verfügung stehen, solange er das Skript nicht bis zu der besagten Stelle hat laufen können.

Fazit

Verglichen mit der rudimentären Konsole, die Microsoft ausliefert, ist PowerShellPlus ein Quantensprung für die alltägliche Arbeit. Die Vorschläge bei der Eingabe funktionieren zwar noch nicht in allen Konstellationen, erleichtern aber in vielen Standardsituationen die Erstellung von Befehlsfolgen und Skripten – gerade dann, wenn man in Ermangelung von Commandlets auf die .Net- oder WMI-Klassenbibliothek zurückgreifen muss.

Viel zu kurz ist leider bislang die mitgelieferte Hilfe. Einige Funktionen (z. B. die Schaltflächen im Properties-Fenster) sind dort gar nicht beschrieben und da es keine Tooltips gibt, kann der Anwender nur ausprobieren, was passiert. Dennoch gehört die PowerShellPlus schon jetzt auf den Rechner eines jeden Administrators. (WM)

DR. HOLGER SCHWICHTENBERG

unterstützt mit seiner Firma IT-Visions.de Unternehmen beim Einsatz von .Net und ist Autor zahlreicher IT-Fachbücher.

Literatur

[1] Holger Schwichtenberg; PowerShell-Tutorial I-IV; *iX* 7/07 bis 11/07

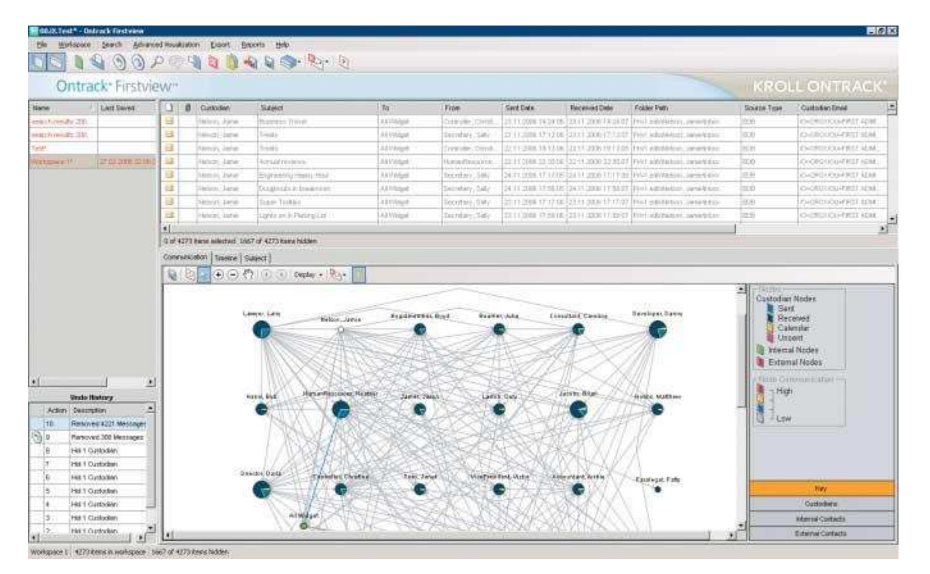
Daten und Preise

Produkt: PowerShellPlus 1.0.2
IDE für Microsofts PowerShell
Hersteller: Shell Tools LLC
Entwickler: Dr. Tobias Weltner
Bezugsquelle: www.powershell.de
Preis: pro User 94 Euro (kostenfrei für den nichtkommerziellen Einsatz)

iX-Wertung

⊕ Eingabeunterstützung für Commandlets und Klassen
⊕ Skript-Editor und Debugger
⊕ anpassbare Konsole
⊖ unzureichende Dokumentation
⊖ gelegentlich Fehler in der Eingabeunterstützung





Firstview: Komplexe Mailbeziehungen sichtbar machen

Der große Überblick

Sebastian Krause

Die neue Version der E-Mail-Analysesoftware Ontrack Firstview soll Anwälte und Ermittler im Rahmen von unternehmensinternen Ermittlungen sowie Zivil- und Strafprozessen bei der Untersuchung umfangreicher E-Mail-Kommunikation unterstützen.

Hinweise auf Fehlverhalten von Mitarbeitern erhält man in vielen Fällen aus der Analyse des Informationsflusses der elektronischen Kommunikation, im Wesentlichen E-Mail. Antworten auf die Fragen, wer mit wem wann wie oft über welche Themen kommuniziert hat, lassen Rückschlüsse auf potenziell beweiskräftige Kommunikationsbeziehungen zu.

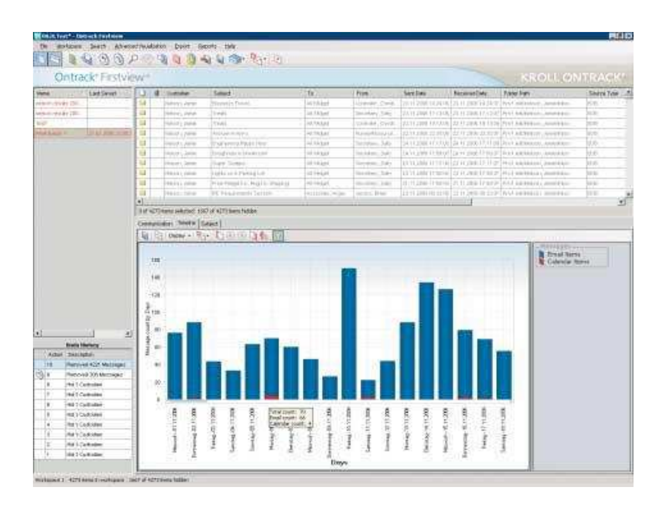
Entsprechende Analysewerkzeuge dürfen allerdings nur gemäß den rechtlichen Rahmenbedingungen eingesetzt werden. So dürfen Arbeitgeber sie nur benutzen, wenn ein hinreichender Verdacht auf ein Vergehen besteht, der Betriebsrat eingebunden ist und die Überwachung nur vorübergehend erfolgt. Strafverfolgungsbehörden müssen in der Regel eine richterliche Anordnung zur Beschlagnahme oder Durchsuchung vorweisen. Problematisch in beiden Fällen ist es, wenn private E-Mails betroffen sind, dann sind die gesetzlichen Hürden für den Einsatz einer solchen Software am höchsten.

Die gerade in Version 2.0 erschienene Analysesoftware Firstview des Datenrettungs- und Forensik-Dienstleisters Kroll Ontrack unterstützt neben der Messaging-Plattform Microsoft Exchange nun auch Lotus Notes. Es lassen sich sowohl Exchange-Datenbanken (.edb) als auch persönliche Postfachspeicher (.pst) einbinden. Wenn man diese Quellen als Fall in die Analysesoftware importiert, listet das Programm alle enthaltenen Nachrichten in Tabellenform in einem Arbeitsbereich zur weiteren Bearbeitung auf.

Dem Ermittler stehen zwei wesentliche Methoden zur Verfügung, um die Spreu vom Weizen zu trennen. Zum einen kann er die Suchfunktion verwenden, um gezielt klassische E-Mail-Eigenschaften wie Empfänger, Absender et cetera zu recherchieren. Eine Suche nach Zeichenketten in E-Mail-Headern ist nicht vorgesehen. Die Ergebnisse kann man innerhalb der Suchfunktion betrachten oder in einen Arbeitsbereich exportieren. Dadurch lassen sie sich insbesondere für die Reporterstellung geeignet gruppieren. Eine Drag & Drop-Funktion würde den Bedienkomfort deutlich erhöhen. Die neuen Analysefunktionen, die unter anderem eine thematische Suche nach inhaltlich ähnlichen E-Mails erlauben sollen, ließen sich in der zur Verfügung gestellten Testsoftware nicht initialisieren und konnten somit nicht getestet werden. Der Hersteller konnte keine Hilfestellung leisten.

Nur Relevantes sichtbar machen

Die zweite Methode besteht darin, die im jeweils aktuellen Arbeitsbereich enthaltenen Nachrichten nach Kommunikationsbeziehungen, zeitlicher Verteilung und Betreff zu untersuchen. Dabei ist besonders hilfreich, dass die Darstellungen mit den zuvor erwähnten Tabellen in Beziehung stehen. Klickt der Ermitt-



Firstview kann darstellen, wie viele Mails des aktuellen Arbeitsbereichs zu den jeweiligen Zeitpunkten (Skala einstellbar nach Stunden, Tage, Wochen etc.) übertragen wurden (Abb. 1).

ler beispielsweise auf eine Verbindung zwischen zwei Kommunikationspartnern, zeigt Firstview in der Tabelle automatisch nur noch alle diesen Nachrichtenweg betreffenden Nachrichten an. Hält er den Mauszeiger über ein Objekt in den Diagrammen, werden statistische Informationen eingeblendet. Damit der Benutzer sich auf die ermittlungsrelevanten Kommunikationsbeziehungen konzentrieren kann, kann er einzelne Objekte ausblenden oder gänzlich aus dem Arbeitsbereich entfernen.

Die Zeit bringt es an den Tag

Untersuchungen auf Auffälligkeiten im zeitlichen Verlauf der E-Mail-Kommunikation, beispielsweise mit einem bestimmten Betreff, kann der Ermittler anschaulich über die Darstellung in Zeitlinien durchführen. In der weiteren Behandlung von Auffälligkeiten fehlt es der Software jedoch an Möglichkeiten, diese zu markieren und ihre Relevanz zu dokumentieren. Der Ermittler kann lediglich auffällige Nachrichten in aussagekräftige Arbeitsbereiche gruppieren, eine Bookmark-Funktion ist nicht vorhanden.

Firstview ermöglicht den Export von persönlichen Postfächern aus den eingebundenen Exchange-Datenbanken. Einzelne Nachrichten kann man nicht exportieren. Das wäre jedoch wünschenswert, da der Ermittler mit der Analysesoftware nicht auf die Header-Informationen von E-Mails zugreifen kann und gegebenenfalls weitere Werkzeuge hinzuziehen muss. Es bleibt der Umweg über die persönlichen Postfächer.

Im Wesentlichen beschränken sich die Berichtsfunktionen auf den jeweiligen Fall beziehungsweise den Arbeitsbereich zusammenfassende, statistische Reports, deren ansprechend und übersichtlich dargestellte Inhalte nur in geringem Maße anpassbar sind. Auch hier fehlt die Integration von Bookmarks.

Die übersichtliche und verständliche Darstellung komplexer Kommunikationsbeziehungen (siehe Aufmacher) ist außerdem für die Präsentation der Untersuchungsergebnisse insbesondere an fachfremde Personen vorteilhaft. (ur)

iX-Wertung

⊕ übersichtliche Darstellung komplexer Kommunikationen

⊕ Verknüpfung der Analysefunktionen

⊕ ausführliche Reports

⊖ keine Erstellung von Bookmarks

⊖ keine Darstellung von Header-Inhalten

⊖ Export einzelner E-Mails nicht möglich

Daten und Preise

Kroll Ontrack

Website: www.krollontrack.de/ontrackfirstview

Produkt: Ontrack Firstview

Preis: 6100 € netto

SEBASTIAN KRAUSE

ist Security Consultant bei der Berliner HiSolutions AG.

Webentwicklungsumgebung Aptana Studio 1.1

Studiosus

Bernhard Steppan

Eclipse verbindet man meistens mit Java-Entwicklungsumgebungen. Nicht immer zu Recht, wie einer der derzeit leistungsstärksten Web-Editoren zeigt.

Anhängern des als Java-IDE bekannten Eclipse bietet Aptana jetzt ein Entwicklungspaket für diese IDE an. Aptana Studio ist in einer kostenfreien Community und einer Professional Edition verfügbar. Beide Versionen basieren auf Eclipse 3.2.2. Entwickler können sie entweder in Form von Plug-ins für eine bestehende Eclipse-Installation oder als Komplettversion mit einem vorkonfiguriertem minimalen Eclipse installieren. Sie haben daher die Wahl, ob sie eine schon konfigurierte IDE ausbauen wollen oder eine spezialisierte Webentwicklungsumgebung benötigen.

Der große Vorteil einer Entwicklungsumgebung, die auf Eclipse basiert, zeigt sich schon bei den ersten Schritten mit der neuen Umgebung. Trotz der Vielzahl an neuen Fenstern und Funktionen findet man sich als mit Eclipse erfahrener Entwickler sofort zurecht und benötigt vergleichsweise wenig Einarbeitungszeit. Vermisst man das eine oder andere Feature, lässt es sich mit dem Update-Manager in Sekunden nachinstallieren. Alle wichtigen Update-Sites für eine PHP-Umgebung, RadRails, Unterstützung für Adobes AIR sowie für iPhone und iPod touch, Professional Studio, Versionskontrollsysteme wie Perforce und Subclipse (Subversion) sind vorkonfiguriert.

Wenn man von einer solchen Entwicklungsumgebung spricht, stellt sich immer die Frage, wie viele Plug-ins aus den Eclipse-Frameworks stammen und wie viele der Hersteller neu entwickelt hat. Wer der Professional Version von Aptana Studio unter die Haube sieht, ist angenehm überrascht, dass knapp 40 Prozent der installierten Plug-ins vom Hersteller selbst stammen. Aptana Studio ist also eine eigenständige Neuentwicklung auf Eclipse-Basis und nicht einfach nur eine schöne Zusammenstellung vieler Open-Source-Plug-ins.

Beliebige Kombinationen von Frames

Wie bei Eclipse gewohnt, gliedert sich die Arbeitsoberfläche der Webentwicklungsumgebung in einen zentralen Editorbereich, der von mehreren Sichten eingerahmt ist und nach Belieben verändert werden kann. Vorkonfiguriert sind zwar nur zwei Perspektiven, sie lassen sich aber beliebig klonen und danach nach eigenen Wünschen umkonfigurieren und speichern. Auf diese Weise kann der Entwickler schnell mehrere maßgeschneiderte Arbeitsumgebungen erzeugen, zwischen denen er per Mausklick umschalten kann, beispielsweise eine spezielle Umgebung für die Teamarbeit oder eine andere für die Fehlersuche.

Der Quellcode-Editor bietet für Javascript, HTML, CSS, PHP und XML Standard-Features wie Syntaxhervorhebung, Zeilennummerierung, Codefaltung und eine umfangreiche Programmierhilfe. Ist eine HTML- oder PHP-Datei in Bearbeitung, besitzt das Editorfenster im oberen Bereich drei Register. Sie erlauben es, zwischen HTML-, Javascript- und CSS-Funktionen zu springen. In den Projekteinstellungen kann der Entwickler unterschiedliche Konfigurationen für die Formatierung von Javascript-, HTML-, CSS- und XML-Dateien wählen.

Eng gekoppelt mit dem Codeeditor ist die Browser-Vorschau. Sie ist für die üblichen Browser, die unter dem Betriebssystem zur Verfügung stehen, vorkonfiguriert. Unter Windows sind das der Internet Explorer und Firefox, beim Mac OS X Safari und Firefox. Weitere Browser lassen sich manuell konfigurieren. Außerdem steht noch eine iPhone-Vorschau zur Verfügung. Sie gestattet es, eine Webseite so anzuzeigen, wie sie das iPhone darstellen würde. Per Mausklick wechselt man von der Vertikal- in die Horizontaldarstellung. In den Grundeinstellungen der Entwicklungsumgebungen hat man bei der Option „iPhone Plugin" die Auswahl zwischen dem Safari und dem Firefox-Browser. Letztere Option ist natürlich sinnlos und verursacht prompt einen Fehler, da das iPhone beziehungsweise der iPod touch nur über eine angepasste Version von Safari und nicht über den Firefox verfügen.

Freunde komfortabler Webdesigner wie Dreamweaver oder Expression Web dürften einen WYSIWYG-Editor vermissen. Sein Fehlen hängt vermutlich damit zusammen, dass die Zielgruppe des Werkzeugs in erster Linie Webprofis sind, die der Codegenerierung dieser Werkzeuge ohnehin nicht trauen und ihren Code per Hand optimieren. Dass man dennoch nicht auf ein Mindestmaß an Komfort verzichten muss, dafür sorgen einige Codevorlagen (Snippets). Hier sollte man jedoch nicht allzu viel erwarten. Das Snippet für eine HTML-Tabelle etwa ersetzt keinen komfortablen visuellen Tabelleneditor. Und so sieht es auch mit Image Maps aus, die man ebenfalls per Hand gestalten darf.

Integrierte iPone-Entwicklung

Der Test einer Site beziehungsweise einer einzelnen Seite funktioniert ähnlich wie bei einer Java- oder C++-Entwicklungsumgebung. Mit „Start" erscheint



Die integrierten Funktionen zur iPhone-Entwicklung erlauben eine genaue Vorschau der Seite für das iPhone und das direkte Ausführen des Codes auf dem Mobiltelefon.

die aktive Seite im voreingestellten Browser, den Aptana Studio automatisch startet, sofern er nicht schon aktiv ist. Mehrere Ausgangskonfigurationen für verschiedene Browser oder andere Einstellungen lassen sich anlegen. Der Entwickler kann iPhone- und iPod-Touch-Sites dank eines iPhone Application Servers direkt auf dem Gerät ausführen. Jede Änderung im Quelltext führt umgehend zu einer Aktualisierung der Seite auf dem Endgerät.

Für die Bearbeitung von Javascript-Programmen und Ajax-Sites steht ein leistungsfähiger Javascript-Debugger zur Verfügung, den eine Debug-Perspektive steuert. Die unter „Start“ definierten Konfigurationen werden übernommen. Der Debugger bietet ähnlichen Komfort wie eine Java-Entwicklungsumgebung. Das heißt, Breakpoints lassen sich setzen, Variablen überwachen sowie ändern. Damit das zum Beispiel mit Firefox klappt, installiert Aptana sowohl Firebug als auch ein eigenes Debugger Add-on für den Browser. Dies Modul lässt sich direkt im Browser konfigurieren. Der Javascript-Debugger für den Internet Explorer ist nur in der Professional Edition vorhanden.

Das Site-Management funktioniert ähnlich dem Projektmanagement der Java-IDE von Eclipse. Alle Projekte erscheinen in einem Projekt-Explorer, einer Sicht namens „Project“. Hier kann der Designer Projekte anlegen, löschen, im- und exportieren sowie neue Dateien anlegen. „Working Sets“ können ebenfalls gebildet werden. Unter ihnen lassen sich bei einer Eclipse-IDE Subprojekte definieren. Das ist beispielsweise praktisch, wenn man in einem großen Projekt nur an einem bestimmten Abschnitt wie einem Einkaufskorb arbeitet.

Hat man ein „Working Set“ definiert, das exakt die Dateien umfasst, die zur Teilaufgabe gehören, kann man zwischen dieser Sicht und der kompletten Projektsicht auf Knopfdruck wechseln. Man kann verschiedenen Working Sets anlegen, die helfen, die Übersicht bei größeren Projekten nicht zu verlieren und nur das zu sehen, was man momentan tatsächlich benötigt. Das Site-Management ist leider nicht so leistungsfähig wie das Projektmanagement in der Java-IDE von Eclipse. So sind beispielsweise die Filter für diese Sicht eher dürftig ausgefallen. Geschlossene Projekte oder für Aptana nicht editierbare Dateien lassen sich daher nur über Working Sets ausblenden.

Refactoring nicht automatisiert

Auffällig ist, dass es keine Refactoring-Funktionen gibt, mit denen sich Projekte unter Wahrung der Konsistenz umstrukturieren lassen. Dass diese Funktionen sinnvoll wären, merkt man beispielsweise, wenn man eine referenzierte CSS-Datei innerhalb eines Projekts umbenennt. Aptana Studio zieht die Umbenennung in den HTML-Dateien, die diese Datei verwenden, nicht automatisch nach. Die Sicht „File References“ liefert nicht unbedingt zuverlässige Ergebnisse, wenn es um die Vernetzung von Dateien geht. Aus diesem Grund ist es nicht weiter verwunderlich, dass es keine Baumansicht einer Site gibt, wie sie beispielsweise Go Live so hervorragend liefert.

Wer seine fertige Site auf einen Server oder ein anderes Laufwerk übertragen und synchronisieren will, bekommt wieder erstklassige Unterstützung. Sie drückt sich in einer übersichtlichen Sicht, einem ebensolchen Konfigurationsdialog und in den unterstützten Standardprotokollen FTP, SFTP, FTPS aus (die letzten beiden nur in der Professional Edition). Eine Vielzahl von Beispielen und mitgelieferten Bibliotheken (Dojo, Mochikit, Scriptaculous) sowie unterstützte Techniken (Ajax, X/HTML, Adobes AIR, Ruby, XML) runden neben der hervorragenden Onlinedokumentation den Eindruck einer außergewöhnlichen Entwicklungsumgebung ab.

iX-Wertung

Aptana Studio

⊕ plattformunabhängig
⊕ Funktionsumfang
⊕ Dokumentation
⊕ Preis

⊖ Site-Management

Fazit

Mit seiner robusten Eclipse-Basis, dem modularen Aufbau und der Plattformunabhängigkeit ist Aptana Studio im codezentrierten Bereich der Webentwicklung eine der besten Umgebungen. Selbst Dreamweaver und Expression Web können nicht überall Paroli bieten. Um mit den Marktführern in allen Bereichen gleichzuziehen, fehlen Aptana Studio allerdings noch einige Funktionen. Das sind nicht nur die erwähnten visuelle Editoren für Image Maps oder Tabellen, sondern vor allem ein wesentlich umfangreicheres Site-Management. (hb)

BERNHARD STEPPAN

arbeitet als Softwareentwickler und freier Autor in Bad Homburg.

Lieferumfang und Preise

Produktname: Aptana Studio
Version: 1.1
Homepage: www.apatana.com
Installationsmedium: Download
Lizenz: Einzellizenz
Speicherbedarf: circa 512 MByte RAM, 200 MByte HD
Hardware-Anforderungen: PC mit mindestens 700 MHz Pentium 4, Mac G5
Betriebssystem: Windows, Mac OS X ab 10.4, Linux mit GTK
Java-Laufzeitumgebung: ab 1.5
Eclipse: 3.2.x (bei der Vollinstallation im Lieferumfang)
Dokumentation: Onlinehilfe, Videos, Handbücher
Preis: kostenfrei (Community Edition), 99 US-$ (Professional Edition)
Anbieter: www.aptana.de

Verschlüsselter Datenverkehr mit Safenets Ethernet Encryptor



Fire on the Wire

Michael Hamm

Ethernet-Encryptoren von Safenet verschlüsseln den Netzwerkverkehr auf Layer 2 und schlagen damit hinsichtlich der Übertragungskapazität in manchen Anwendungsbereichen das langsamere IPSec.

Öffentliche, stadtumspannende Metropolitan Area Networks (MAN) bieten eine attraktive und kostengünstige Alternative zur unternehmensweiten Vernetzung. Zu beobachten ist, dass bei diesen Netzwerken mehr und mehr die bisher eingesetzten Wide-Area-Network (WAN)-Techniken durch das billigere und robustere Ethernet verdrängt werden.

Den Schutz der Daten realisiert man heute üblicherweise durch VPNs, basierend auf IPSec-Gateways. Bei dieser Technik kämpfen Administratoren mit umfangreichen Konfigurationsarbeiten und einem Verlust von Bandbreite durch Overhead bei den IP-Paketen. Hier will Safenet mit seinen auf Netzwerk-Layer 2 arbeitenden Geräten „Ethernet Encryptor“ (SEE) punkten.

Beim Einsatz ist unbedingt darauf zu achten, dass ein SEE-Paar nur in einem nicht gerouteten Netzwerk miteinander kommunizieren kann. Modifikationen am Datenverkehr wie das Ändern der Reihenfolge der Frames oder das Routen der Daten mit einhergehendem Ändern der MAC-Adressen werden nicht unterstützt.

Man integriert daher die Geräte via Plug & Play außerhalb des äußeren Routers aufseiten des MAN-Providers transparent in ein bestehendes Netzwerk (Abb. 1). Damit dies reibungslos verläuft, ist eine entsprechende Vorkonfiguration erforderlich.

Verschiedene Anschlüsse möglich

Ein SEE verfügt an der Rückseite über zwei Ethernet-Schnittstellen, wahlweise 10, 100 oder 1000 MBit. Dem Autor standen leider nur zwei 100-MBit-Geräte zum Testen zur Verfügung, die schnelleren Geräte konnte der Hersteller zu diesem Zeitpunkt nicht liefern.

Deren Netzwerkkarten sind mit einer SFP-Schnittstelle (Small Form-Factor Pluggable) ausgestattet. So kann wahlweise ein RJ-45-Stecker, ein optisches Single- oder ein optisches Multi-Mode-Modul die Verbindung herstellen.

Den mit „LOCAL“ bezeichneten Ethernet-Anschluss verbindet man mit der vertrauenswürdigen Seite des Netzwerkes, den mit „NETWORK“ gekennzeichneten mit dem öffentlichen MAN. Grundsätzlich ist sowohl ein- als auch ausgehender Netzwerkverkehr am lokalen Interface unverschlüsselt. Ein- und ausgehender Verkehr am externen Interface ist je nach Policy unverschlüsselt oder verschlüsselt. Zur Verschlüsselung kommt der AES-Algorithmus mit 256 Bit zum Einsatz. Er verschlüsselt die gesamten Nutzdaten eines Ethernet-Frames. Erfreulicherweise ändert sich die Frame-Größe dabei nicht, sodass kein Overhead entsteht.

SEEs arbeiten immer paarweise zusammen. Jedes Paar benutzt sein eigenes geheimes Schlüsselpaar. Damit ein Ethernet Encryptor weiß, welcher Schlüssel zu benutzen ist, labelt er die MAC-Adressen. Bei eingehenden Frames am lokalen Port markiert er die Ziel-MAC-Adresse des Frames als Remote-MAC-Adresse und bei eingehenden Frames am externen Port die Source-MAC-Adresse des Frames als Remote-MAC-Adresse.

Zuvor ist mittels Zertifikaten eine Vertrauensbeziehung zwischen den Encryptor-Geräten herzustellen – was eine Teilaufgabe des Safenet Security Management Center (SMC) ist.

Darstellung komplexer Landschaften

Beim Security Management Center handelt es sich um eine Software-Suite zur Remote-Verwaltung von sicherheitsrelevanten Netzwerkkomponenten wie dem Ethernet Encryptor. Sein Hauptfenster besteht aus einer visuellen Darstellung der verwalteten Komponenten (Map) (Abb. 2). Maps lassen sich verschachteln, wodurch auch komplexe Topologien übersichtlich dargestellt werden können. Jedes Objekt hat seine eigene Submap mit den zugehörigen Funktionen (Abb. 3).

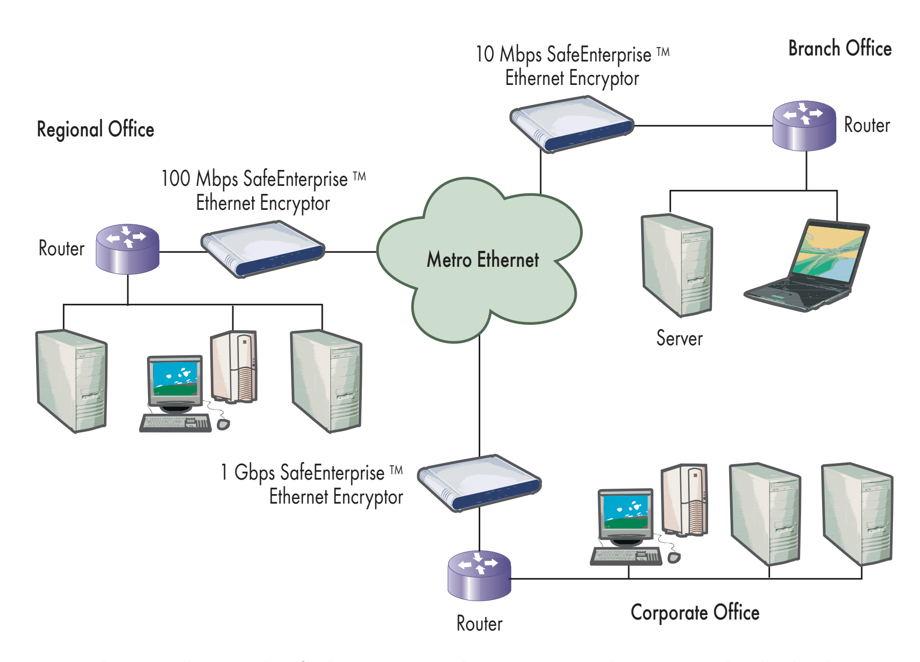
Ein wichtiger Bestandteil der Software ist eine Certificate Authority (CA). Benötigte Dienste wie LDAP-Server und MySQL-Datenbank liefert sie gleich mit.

SMC empfiehlt der Hersteller für Solaris oder Windows 2000/2003 Server. Es besteht aus dem eigentlichen Management-Center und der Management-Konsole, dem grafischen Benutzer-Interface. Die beiden Komponenten lassen sich auf demselben System installieren (Stand-alone), die Management-Konsole überdies auf bis zu fünf zusätzlichen Rechnern.

Weitere Installationsalternativen sind ein Hot-Standby-Server-Szenario, bei dem die Datenbanken regelmäßig auf einen zweiten Server repliziert werden (DRF Data Replication with Failover Mode), sowie das Multi-Manager-Szenario, bei dem mehrere SMC-Server in verschiedenen Standorten installiert sind. Die Datenbanken muss der Systemverantwortliche in diesem Fall allerdings manuell synchronisieren.

SMC unterstützt eine komplexe Rechteverwaltung (OrBAC – Organization Based Access Control) für Administratoren. Auf oberster Ebene kann er Organisationen definieren. Neu angelegte Benutzer-Accounts sind immer einer dieser Organisationen zuzuweisen.

Neben der Aufteilung nach Organisationen unterstützt das System außerdem ein Rollenkonzept für Anwender. Neben den bestehenden Rollen Operator, Techniker, Manager und Admin – mit jeweils vordefinierten Zugriffsrechten – können auch eigene Rollen definiert werden.



Das robuste Ethernet läuft dem Unternehmens-WAN den Rang ab, doch ohne Sicherheitsmaßnahmen geht es nicht. Der Ethernet Encryptor wird transparent ins Netzwerk integriert und ver- beziehungsweise entschlüsselt den ein- und ausgehenden Datenverkehr an der Unternehmensgrenze (Abb. 1).

Vorbereitungen für den Einsatz

Bei der Vorinstallation kommt das Front Panel zum Einsatz (siehe Aufmacher). Hier findet sich neben einem Ethernet-Anschluss ein serieller Konsolenport, ein Tastenblock und ein Flüssigkristall-Display für zwei Zeilen à 20 Buchstaben. Am seriellen Konsolenport steht ein Command Line Interface mit einem Login Prompt zur Verfügung. Der Ethernet-Anschluss dient zur Remote-Verwaltung via SMC im Standard-Outband-Management-Modus.

„Plan B" bei Ressourcen-Knappheit

Sollte der Provider aus technischen Gründen wie Ressourcenknappheit kein separates Management-Interface unterstützen, kann der SEE später auch im Inband-Management-Modus betrieben werden, wobei der Management-Datenverkehr zusammen mit dem normalen Benutzerverkehr über die Netzwerkschnittstellen an der Rückseite (Back Panel) übertragen wird.

Die nötigen Informationen wie IP-Adresse, Netzmaske und Standard-Gateway sind beim Netzwerk-Provider zu erfragen. Dynamische IP-Adressen etwa via DHCP unterstützen die Ethernet Encryptors nicht. Die erhaltenen IP-Daten gibt der Administrator via Tastenblock am Front Panel ein. Des Weiteren muss er das korrekte Datum sowie die ungefähre Uhrzeit eingeben.

Im Folgenden ist eine Vertrauensbeziehung zwischen SMC und SEE mittels eines gültigen Zertifikates herzustellen. Hierzu sind wechselseitig Aktionen von einem Administrator an der SMC und einem Administrator am SEE durchzuführen. War das erfolgreich, wird das Zertifikat auf dem Encryptor installiert. Von diesem Zeitpunkt an kann und sollte der Administrator das Gerät vom SMC aus remote verwalten.

Ein SEE unterstützt bis zu 30 Administratoren, denen eine der beiden Rollen Administrator oder Operator zuzuweisen ist. Im Gegensatz zu Administratoren, die vollen Zugriff auf das System haben, kann ein Operator die Konfigurationsparameter nur überwachen. Nicht zu verwechseln sind SEE- mit SMC-Administratoren.

Getestete Geschwindigkeit

Von besonderem Interesse in diesem Test war die Überprüfung des versprochenen Geschwindigkeitsgewinns gegenüber IPSec durch die overheadfreie Verschlüsselung auf Layer 2.

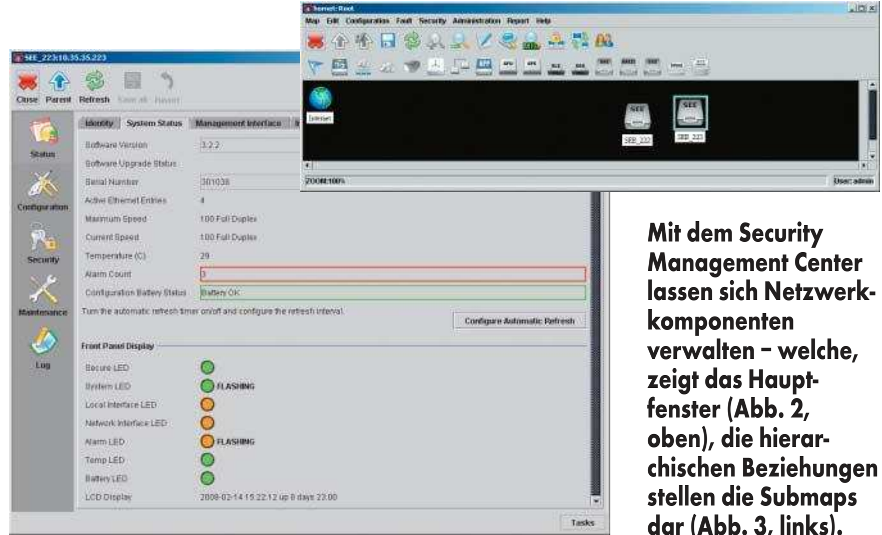
Belegen soll das zwar die Studie „Comparative Performance of Layer 2 and IPSec Encryption on Ethernet Networks", die im Oktober 2006 am Rochester Institute of Technology durchgeführt wurde. Da jedoch Safenet diese Studie finanziert hat, wollte *iX* sich nicht blind darauf verlassen.

Beim *iX*-Test wurden lediglich zwei PCs über zwei SEEs vernetzt. Einer wurde jeweils am „LOCAL"-Interface einer SEE angeschlossen, die beiden „NETWORK"-Ports der Verschlüsselungsgeräte wurden mit einem X-Kabel verbunden. Zum Testen der Geschwindigkeit setzte der Autor das Tool *netio* von Kai Uwe Rommel ein (www.nwlab.net/art/netio/netio.html).

In einem ersten Test maß er die Geschwindigkeit ohne Verschlüsselung. Hierzu wurde die globale Policy auf „Bypass All" gesetzt. Tatsächlich war der Datendurchsatz über TCP/IP höher (92 MBit/s) als bei einem handelsüblichen Hub (86 MBit/s), an dem ansonsten keine weiteren Geräte angschlossen waren.

In einem weiteren Test mit aktivierter Verschlüsselung konnte in der Tat keine spürbare Reduzierung der Bandbreite festgestellt werden. Die Wirespeed-Verschlüsselung für die 100-MBit-Variante bestätigte sich im Test. Schade nur, dass dieser nicht mit 1 GBit/s durchgeführt werden konnte.

Der Vorteil gegenüber IPSec kommt vor allen Dingen bei Anwendungen mit vielen, aber kleinen Datenpaketen – etwa bei VoIP – zum Tragen. Hier kann der IPSec-Overhead, der möglicherweise bei einer FTP-Übertragung nur bei 3-5 Prozent liegt, auf bis zu 40 % steigen.



Mit dem Security Management Center lassen sich Netzwerkkomponenten verwalten – welche, zeigt das Hauptfenster (Abb. 2, oben), die hierarchischen Beziehungen stellen die Submaps dar (Abb. 3, links).

In der entsprechenden SEE-Submap des SMC kann man Wartungsarbeiten durchführen und den Systemstatus überwachen. Hier werden auch Logs wie das Audit-Log überprüft, das eine Liste der vom Administrator durchgeführten Aktivitäten und sicherheitsbezogener Systemmeldungen enthält. Das Event-Log verzeichnet alle Systemmeldungen. Gravierende Meldungen, die auf einen Defekt, ein Sicherheitsproblem oder eine tiefgreifende Änderung am System hinweisen, finden sich im Alarm-Log.

... und Action!

Alarme müssen von einem Administrator bearbeitet, zumindest als registriert markiert werden. Solange es unbeantwortete („unacknowledged“) Alarme gibt, visualisiert das eine rote LED am Front Panel des Encryptors.

Sind die SEEs korrekt ans Netzwerk angeschlossen, sollten sie dank der ausgestellten Zertifikate und der vertrauenswürdigen CA auf Anhieb zusammenarbeiten. SEE kann Layer-2-Frames auf drei Arten behandeln:
– „Discard“: Der Encryptor verwirft den Frame.
– „Bypass“: Er leitet den Frame ohne weitere Veränderungen weiter.
– Encrypt: Der Frame wird verschlüsselt.
Was im Einzelnen zu tun ist, entscheidet sich anhand einer hierarchischen Security Policy. Der Administrator kann gobale, Layer-2- protokollbezogene und MAC-Adressen-bezogene Regeln definieren.

Fazit

Zwar vermitteln die SEEs von der gesamten Konzeption her einen soliden und auf Sicherheit bedachten Eindruck – vom Systemstart an, über die in einer geschützten Umgebung vorzunehmende Vorkonfiguration bis zur anschließenden Fernverwaltung.

Aber eine Vereinfachung der Installation und Wartung gegenüber integralen IPSec-Lösungen konnte der Autor nicht feststellen. Einen klaren Vorteil gegenüber IPSec bietet das Gerät in puncto Durchsatz. Da hier quasi kein Overhead über das Netz transportiert wird, sind spürbar schnellere Verbindungen möglich. Leider stand zum Test kein 1-GBit-Gerät zur verfügung. (ur)

MICHAEL HAMM

ist Ingénieur Sécurité am Centre de Recherche Public Henri Tudor in Luxemburg.

Daten, Preise, Wertung

Produkt: Ethernet Encryptor
Hardware-Appliance zur AES-Verschlüsselung auf Layer 2 mit 10 Mbps, 100 Mbps, 1Gbps
Hersteller: Safenet; www.safenet-inc.com/de
Preise: ab 12 630 € (inkl. MwSt.), SMC-Software ab 3930 € (inkl. MwSt.)

⊕ hoher Datendurchsatz
⊕ durchgängiges Sicherheitskonzept

⊖ nur anwendbar in nicht gerouteten Netzen
⊖ proprietäres Verfahren erfordert immer zwei Geräte

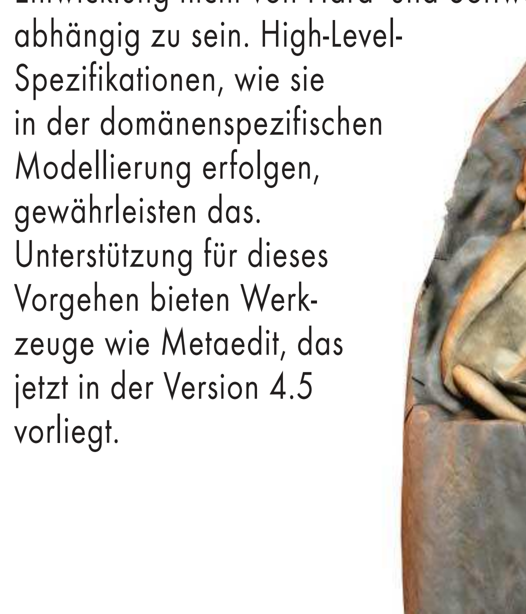


Domänenspezifisches Modellieren mit Metaedit+ 4.5

Facharbeit

Eldar Sultanow

Für Programmierer bedeutet es eine große Freiheit, bei der Entwicklung nicht von Hard- und Softwareplattformen abhängig zu sein. High-Level-Spezifikationen, wie sie in der domänenspezifischen Modellierung erfolgen, gewährleisten das. Unterstützung für dieses Vorgehen bieten Werkzeuge wie Metaedit, das jetzt in der Version 4.5 vorliegt.



Mithilfe der von der Object Management Group spezifizierten Model Driven Architecture (MDA) können Softwareentwickler plattformunabhängige Modelle als Basis für plattformspezifische Code-Generierung erstellen. Die domänenspezifische Modellierung (DSM) verwendet unmittelbar bei der Produktspezifikation die Konzepte der Anwendungsdomäne, und die Generierung der Anwendungen erfolgt auf der Grundlage von High-Level-Spezifikationen. Das bewirkt, dass die Anforderung an Sprache und Generatoren auf lediglich ein Unternehmen beziehungsweise auf eine Anwendungsdomäne beschränkt ist.

In der DSM repräsentieren die Elemente Gegenstände aus der Anwendungs- und nicht aus der Programmierwelt [1]. Die Modellierungssprache orientiert sich an den Abstraktionen und der Semantik der Domäne, sodass die Modellierer direkt mit den Domänenkonzepten arbeiten können. Die Regeln der Anwendungsdomäne kann der Entwickler als Constraints in die DSL (Domain Specific Language) einbinden, sodass es im Idealfall nicht möglich ist, ungültige oder unerwünschte Entwurfsmodelle zu spezifizieren.

Spezielle Werkzeuge wie Metaedit+ der amerikanischen Firma Metacase unterstützen den Entwickler bei der domänenspezifischen Modellierung. Das Tool beinhaltet eine Vielzahl von Standardmodellen, darunter das in Abbildung 1 dargestellte BPMN-Modell (Business Process Modeling Notation), das den typischen Verlauf von Diskussionen beschreibt. Zum Lieferumfang gehören aber auch spezifische Modelle wie das einer auf Nokias Smartphone-Betriebssystem S60 zugeschnittenen Konferenzregistrierungssoftware.

Vom Konzept bis hin zum Generieren

Der Metaedit+ Workflow ist durch zwei Schritte gekennzeichnet: Fachexperten richten die Konzepte und Quelltextgeneratoren ein. Auf dieser Grundlage gestalten Softwareentwickler die Anwendung und generieren den Quelltext. Das Werkzeug integriert sich in die bestehende Applikationsentwicklungsumgebung: Es liest Konfigurationsdateien ein, stellt den Bezug zu Komponentenbibliotheken her und startet Simulationen.

Mithilfe einer Tool-Suite kann der Entwickler zu den Konzepten und Eigenschaften der domänenspezifischen Sprache passende Regeln und Symbole definieren, die er als Metamodell in einem Repository speichert. Dadurch fließen spätere Änderungen direkt in die Modelle und Generatoren ein. Die Software stellt eine fertige Modellierungs- und Code-Generierungs-Umgebung – mit Editoren, Browsern, Mehrbenutzer-Unterstützung – zur Verfügung.

Metaedit+ liegt jetzt in der Version 4.5 SR1 vor und läuft auf allen gängigen Plattformen – unter anderem Windows, Linux, Mac OS X, Solaris und HP-UX. Für den Test wurde die Workbench-Version auf einem AMD 2000+ mit einem Windows Server 2003 installiert.

Benutzeroberfläche wurde runderneuert

Als Erstes fällt die grafische Benutzeroberfläche für Metamodellierung ins Auge, die der Hersteller runderneuert hat. Die Graphenerstellung gestaltet sich einfacher, da sie nicht mehr wie bisher über einen Wizard erfolgt, sondern dialoggesteuert ist. Zusätzliche Fenster erscheinen als Tabs innerhalb des Graph Tool.

Mit dem neuen Icon-Editor kann der Entwickler typenspezifische Icons manuell erstellen und muss nicht mehr auf

die vorgegebenen Symbole zurückgreifen. Alternativ lassen sich zusätzliche Symbole in SVG- und Bitmap-Formaten importieren.

Den Generator hat der Hersteller ebenfalls um einige Funktionen erweitert. So ist jetzt das Iterieren über Variablen und Strings möglich:

```
do $var, do 'foo bar'%spaces
```

Der Programmierer kann das Encoding für (zu generierende) Dateien spezifizieren:

```
filename ... encoding ... write/read
```

und eine verkürzte Syntax erleichtert die einfache Variablenzuweisung und Manipulation:

```
$abc='foo', $abc++, $-abc
```

Das System zur Definition der Codegenerierung unterstützt in der neuen Version Syntax-Highlighting und erlaubt die sofortige Validierung von Generator-Scripts. Ein Debugger erleichtert die Programmierung eigener Generatoren. Über ein Tracing lässt sich generierter Quellcode zu den zugehörigen Modell-Elementen zurückverfolgen.

Der Im- und Export von Modellen und Metamodellen erfolgt jetzt via XML und schließt Diagramme, Matritzen und Tabellenrepräsentationen ein.

Zugriff auf Backends über SOAP

Durch die verbesserte SOAP-API (Simple Object Access Protocol) für Webservices ist die Version 4.5 offener als vorher gegenüber anderen Plattformen wie JEE oder .Net. Ein Zugriff auf Metaedit+-Funktionen ist von beinahe jeder Programmiersprache (Java, C, C++, C#, Visual Basic, Perl et cetera) und Plattform (Windows 98, NT, 2000, XP, Linux, HP-UX, Solaris et cetera) aus möglich.

Metaedit+ generiert für implementierte Funktionen eine WSDL (Web Services Description Language) und stellt Webservice-Schnittstellen öffentlich zur Verfügung. Die API beinhaltet neben Funktionen zum Lesen, Erzeugen und Aktualisieren von Modellelementen solche für die Steuerung einer Anwendung sowie für Scripting- und Simulationsaufgaben.

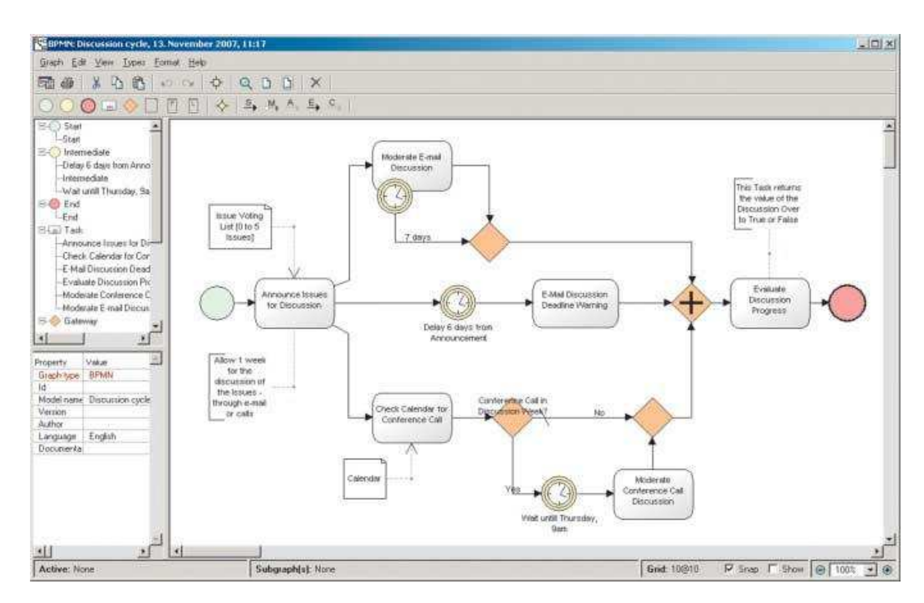
Modelleigenschaften lassen sich durch die Unterstützung von SOA (Service Oriented Architecture) in die Benutzeroberfläche laden, beispielsweise in einen Eigenschaftsdialog. Hierfür muss der Entwickler einen Webservice als Gateway in seine bestehende Umgebung implementieren (etwa in JEE unter Linux oder in .Net unter Windows), der auf die in einer Datenbank abgelegten Modelle beziehungsweise deren Eigenschaften zugreift. Bei einem Fehler während der Übertragungs- oder in der SOAP-Schnittstellendefinition deaktiviert Metaedit+ die betroffenen Felder in der grafischen Oberfläche.

Der Diagramm-Editor bietet eine Baumansicht für alle Objekte einschließlich einer Eigenschaftstabelle für das selektierte Objekt. Diagramme können außer wie bisher im XML-basierten Austauschformat GXL (Graph Exchange Language) als PNG-Dateien (Portable Network Graphics) gespeichert werden.

Hinsichtlich der Datenintegrität war Metacase ebenfalls tätig. Laufen beispielsweise zwei Metaedit+-Instanzen, ist es jetzt ausgeschlossen, dass zwei Personen gleichzeitig dieselben Daten manipulieren. Die zuerst gestartete Instanz blockiert geöffnete Modelle, sodass sie für Dritte nur lesbar sind.

Fazit

Metaedit+ ist ein erprobtes Werkzeug, das seit Jahren in einer Vielzahl von Anwendungsdomänen zur Automatisierung von Softwareentwicklung zum Einsatz kommt. Die in der Version 4.5 hinzugekommenen Funktionen tragen weiter dazu bei, die für die Softwareentwicklung benötigte Zeit deutlich zu verkürzen. (ka)



Das von Metaedit+ mitgelieferte BPMN-Modell beschreibt den typischen Zyklus einer Diskussion (Abb. 1).

ELDAR SULTANOW

arbeitet als J2EE-Entwickler/Architekt bei der Producto AG in Berlin.

Literatur

[1] Dr. Juha-Pekka Tolvanen, Dr. Steven Kelly; Domänenspezifische Modellierung; Objektspektrum 04/04, S. 30

iX-Wertung

- ⊕ hohe Integrierbarkeit in bestehende IT-Systemlandschaften
- ⊕ breites Spektrum unterstützter Betriebssysteme
- ⊕ hohe Modellabstraktion und Spezialisierbarkeit auf die Fachdomäne
- ⊕ Importmöglichkeit von Graph-basierten Daten (GXL, XMI, MOF)

Daten und Preise

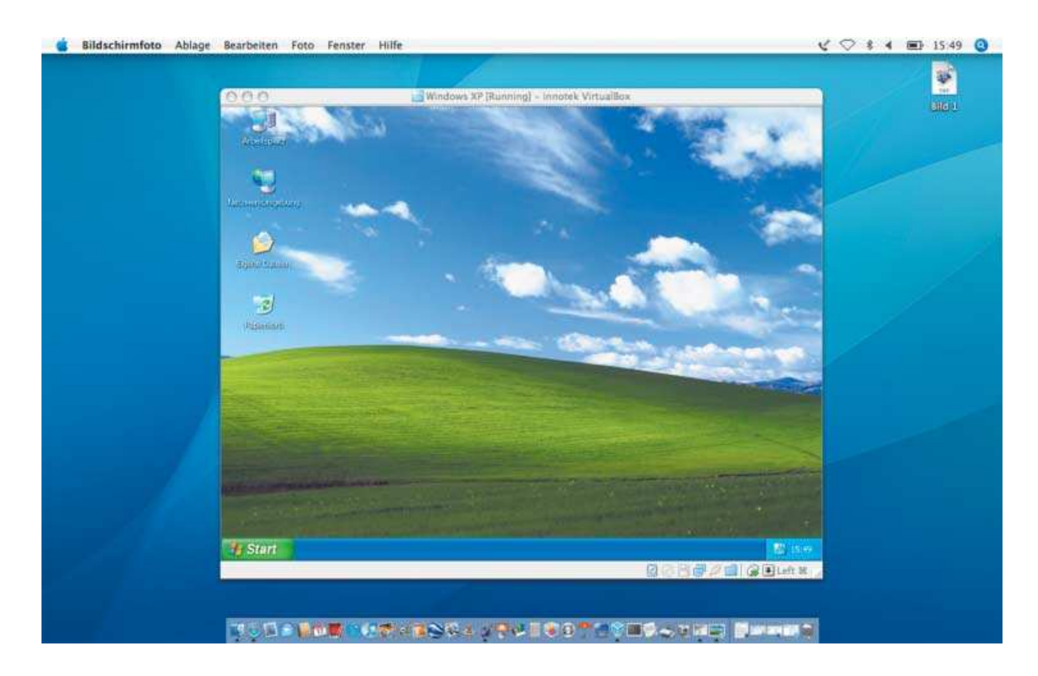
Metaedit+ 4.5

Hersteller: Metacase, www.metacase.com

Softwarevoraussetzungen: Mac OS X, Linux, Windows- oder Unix-Plattform

Hardwarevoraussetzungen: 512 MByte RAM, 60 MByte Festplattenplatz

Preise: Workbench: 9500 €
Modeler: 5500 €
Introductory License: 150 €



Virtualbox für Linux, Mac OS X, Opensolaris und Windows

Springteufel

Markus Franz

Im Schatten des MySQL-Deals hat Sun Microsystems den deutschen Spezialisten für Virtualisierung Innotek gekauft. Dessen Hauptprodukt Virtualbox scheint also eine besondere Rolle zu spielen.

Sucht man als Entwickler oder Administrator heute eine Virtualisierungslösung, steht man vor einem unübersichtlichen Berg von Angeboten: Es gibt mehr als ein Dutzend Produkte aus dem Open-Source-Lager und von kommerziellen Anbietern wie Microsoft oder Parallels.

Grundsätzlich unterscheidet man zwischen Plattform- und Betriebssystemvirtualisierung: Erstere emuliert einen kompletten Rechner und ermöglicht es, Betriebssysteme ohne Modifizierung laufen zu lassen. Letztere erzeugt mehrere geschützte Benutzerbereiche auf ein und demselben Betriebssystem.

Virtualbox – ein Produkt der jüngst von Sun übernommenen Stuttgarter Innotek – gehört zur ersten Kategorie. Es läuft unter Windows, Linux, Mac OS X oder Opensolaris und kann diverse Gastsysteme unverändert betreiben. Als einziger Vertreter dieser Kategorie für x86-Maschinen steht es unter einer offenen Lizenz, in diesem Fall unter der Gnu General Public License (GPL). Die Open-Source-Edition kann daher jeder auf beliebige Weise einsetzen. Daneben gibt es eine kommerzielle Variante, die man nur privat kostenlos nutzen darf. Sie bietet zusätzliche USB-Unterstützung und eine Remote-Desktop-Steuerung für virtuelle Maschinen.

Neue Maschine anlegen

Virtualbox kann man für Windows und Linux in einer stabilen Version auf der Projektseite herunterladen (siehe Kasten „Onlinequellen“). Die angebotenen Binaries für Mac OS X und Opensolaris sind zurzeit noch im Beta-Status und nicht für den produktiven Betrieb gedacht. Das Installieren geht unter allen Betriebssystemen flott von der Hand. Unter Linux, Mac OS X und Opensolaris installiert Virtualbox gleich die benötigten Kernel-Module und -Erweiterungen. Nach einem Neustart läuft nicht nur der Daemon, sondern es existiert auch eine komfortable Oberfläche zur Konfiguration.

Zunächst ist man erfreut, dass Virtualbox die Oberfläche auf Deutsch anbietet. Der Button „Neu“ startet den Assistenten zum Anlegen einer neuen virtuellen Maschine. Grundsätzlich unterstützt Virtualbox jedes Gastbetriebssystem für die Architektur des Host (Auswahl „Unknown“). Allerdings laufen einige Gastsysteme besser, stabiler und eventuell auch schneller, wenn man sie explizit angibt. Unter Solaris etwa funktioniert im generischen Modus die Maus nicht richtig.

Auf der Liste der geladenen Gäste finden sich neben Solaris, Windows, Linux und den freien BSD-Varianten auch Exoten wie DOS, OS/2 Warp und Netware. Mac OS X fehlt derzeit noch, da es trotz Intel-Plattform spezielle Restriktionen von Apple gibt, die sich im Wesentlichen auf das TPM-Modul beziehen. Es lässt sich selbst dann nicht virtualisieren, wenn Virtualbox auf Mac OS X läuft.

Im zweiten Schritt schließt man im Assistenten eine (virtuelle) Festplatte an die Maschine an: Als VDI-Datei (Virtual Disk Image) kann sie die vorgegebene Größe sofort belegen oder dynamisch bis zum Maximum mitwachsen. Aber Obacht: Die Größe der Datei bleibt unabhängig vom Modus nach dem Anlegen unverändert – es sollte also ausreichend Platz vorhanden sein. Allerdings kann man später einer Maschine durchaus weitere VDI-Dateien als zusätzliche Festplatten hinzufügen.

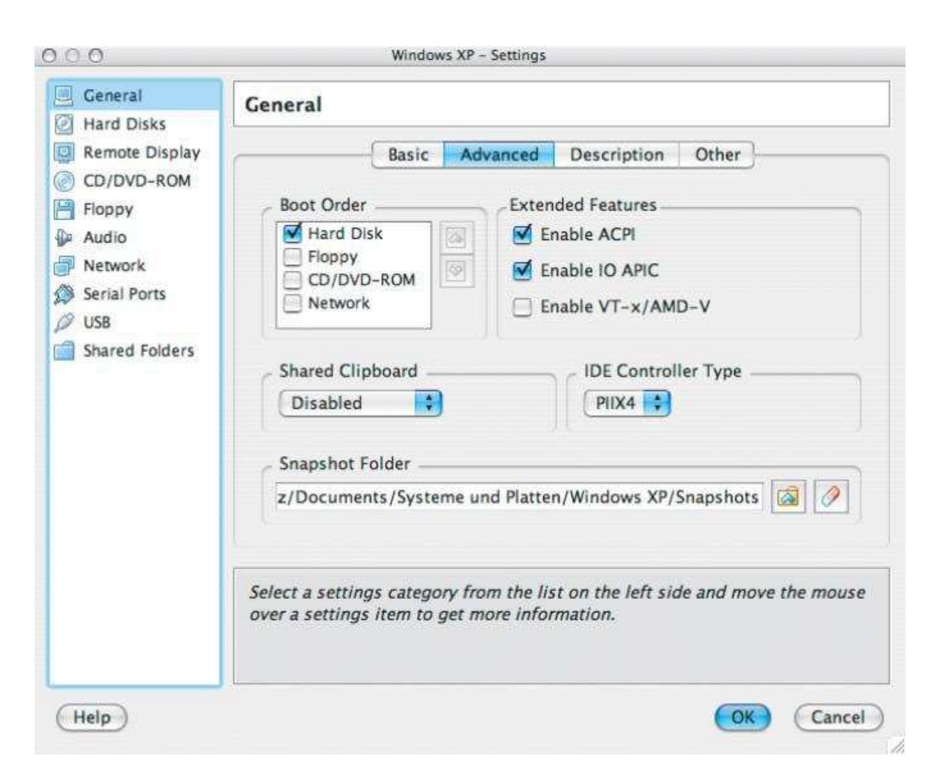
Weitere Optionen für Hardware

Damit man das Gastsystem einrichten kann, bedarf es normalerweise noch einer Installations-CD oder -DVD. Unter „Settings“ erscheint ein Dialog, der umfangreiche weitere Funktionen bietet. Dort lässt sich ein im physischen Laufwerk eingelegter Datenträger an den Gast weiterreichen oder ein ISO-Image direkt einbinden, eine besonders praktische Sache für das Testen von Live-CDs oder -DVDs. Man konfiguriert einfach

eine virtuelle Maschine ohne Festplatte, die nur auf den Datenträger zugreift.

Man kann in den erweiterten Optionen sogar festlegen, dass Virtualbox ATAPI-Kommandos direkt an das Host-Laufwerk durchreicht. In den Settings darf der Admin weitere virtuelle Festplatten hinzufügen und die Boot-Reihenfolge ändern. Außerdem kann er dort die Zwischenablage anpassen. Virtualbox unterstützt ACPI und IO-APIC sowie die Virtualisierungserweiterungen moderner Prozessoren: Es lässt sich sowohl Intels VT-x als auch AMD-V aktivieren. Sofern der Prozessor die Erweiterungen enthält, kann Virtualbox sie direkt nutzen, was mehr Geschwindigkeit, Stabilität und Sicherheit bringt.

Die Verbindung zum Internet geht für ein Gastsystem über das Netzwerk-Interface: Virtualbox gaukelt dem Gast einen Netzwerkadapter der AMD-PCNET-Familie vor (genau: AMD 79C973). Dessen MAC-Adresse lässt sich ebenso beliebig einstellen wie der Status des virtuellen Kabels (verbunden/getrennt). Das Gastsystem kann die Audioausgabe an eine Soundkarte vom Typ AC97 oder Soundblaster 16 weitergeben. Zu guter Letzt stellt Virtualbox einen USB-Controller bereit, den man im Einstellungsdialog aktivieren kann. Aktiviert man den USB-EHCI-Controller, beherrscht Virtualbox sogar das schnelle USB 2.0. Außerdem gibt es die Option, in Virtualbox den Arbeits- und Grafikspeicher einzustellen: Je mehr, desto besser für den Gast – aber schlechter für den Host.



Hard: Virtualbox kann die Erweiterungen von Intels und AMDs Prozessoren für die Virtualisierung nutzen (Abb. 1).

Server mit Remote Desktop

In der Pressemitteilung zum Kauf von Innotek ordnet Sun Virtualbox als Produkt für Entwickler und Heimanwender ein. Es soll das hauseigene Enterprise-Produkt Sun xVM ergänzen. Dabei kann sich Virtualbox auf einem kleinen Server durchaus lohnen: Mit mehreren virtuellen Maschinen erhöht man die Auslastung und sichert die Anwendungsebenen gegeneinander ab. Zu den Besonderheiten zählt, dass Virtualbox für jede virtuelle Maschine einen RDP-Server laufen lassen kann: Im Settings-Dialog unter „Remote Display“ taucht die Option „VRDP-Server“ auf. Man kann dort den Port festlegen, auf dem der Server Verbindungen entgegennimmt – so lassen sich mehrere virtuelle Maschinen parallel über RDP ansteuern. Es empfiehlt sich jedoch, die Authentifizierung nicht über Virtualbox vorzunehmen. Man kann sich stattdessen mit den Benutzerkonten des Gastsystems anmelden.

Für die intensive Nutzung von Virtualbox als professionelle (Server-)Umgebung bietet sich auch die Funktion „Shared Folders“ an: Das sind gemeinsam genutzte Ordner, die sowohl der Host als auch die Gäste nutzen können. Unter Windows findet man das Verzeichnis unter *\\vboxsvr\ordner*. Linux-Nutzer können den Ordner mit dem Befehl *mount –t vboxsf <ordner> <mountpoint>* einbinden.

iX-TRACT

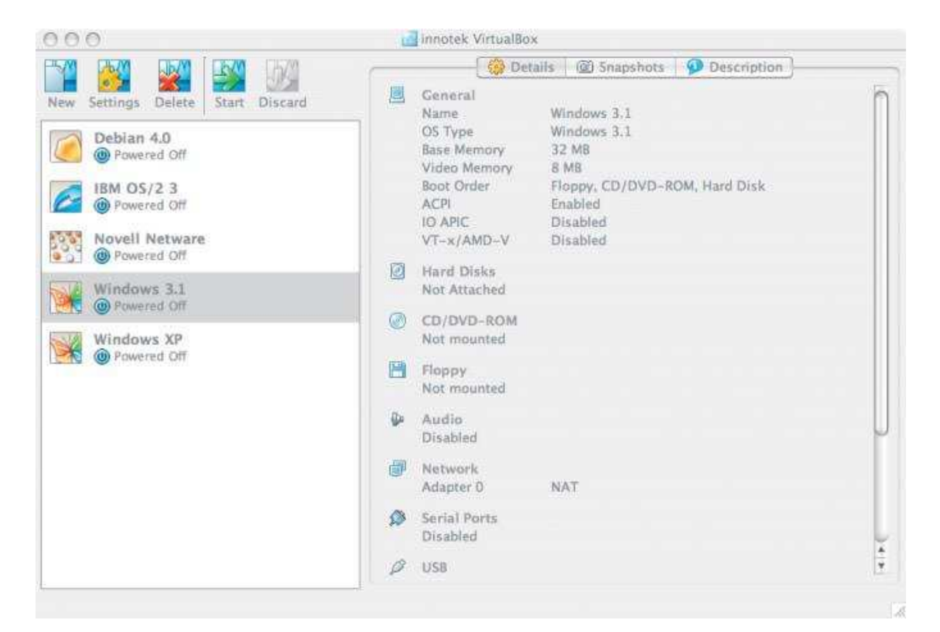
- Virtualbox ist der einzige vollständige Plattform-Virtualisierer aus dem Open-Source-Bereich.
- Die kommerzielle Version ist für den privaten Gebrauch kostenlos.
- Es unterstützt als Host und Gast mit Windows, Linux, Mac OS X und Opensolaris alle gängigen Systeme.

Wer mit dem Gedanken spielt, Virtualbox auf dem Server einzusetzen, dem kommt die Unterstützung für VMware gerade recht: Ein Festplatten-Image aus VMware lässt sich mit dem Programm *vditool* ins VDI-Format konvertieren. So kommt man in den Genuss einer umfangreichen Auswahl an virtuellen Appliances.

Komfort für den Desktop

Für Entwickler und Heimanwender sind dagegen andere Dinge wichtig: Hier zählen vor allem der Komfort und die Performance. Virtualbox kann in diesem Bereich mit Windows oder Linux als Host punkten: Dank der komfortablen, Qt-basierten grafischen Oberfläche kann man auf die Kommandozeile sogar verzichten. Auf Mac OS X befindet sich Virtualbox erst im dritten Beta-Stadium, das am 6. Februar herauskam. Bisher war die Auflösung für das Gastsystem auf maximal 800 × 600 Pixel und 256 Farben begrenzt. Die dritte Beta kann mehr: 32 Bit pro Pixel und Auflösungen bis 1024 × 768 – Virtualbox schließt zur Konkurrenz auf, wenn auch reichlich spät.

Im Test lief die Beta 3 (Virtualbox 1.5.51) auf einem Apple Macbook (Intel Core 2 Duo T7200, 2,0 GHz, 1 GByte RAM) mit Mac OS X 10.4 (Tiger). Hier hat die freie Version von



Exoten: Neben aktuellen Distributionen unterstützt Virtualbox auch Klassiker wie OS/2, Novell Netware oder Windows 3.1 – und bietet sich damit als Träger für Altlasten an (Abb. 2).

Innotek mit den kommerziellen Konkurrenten von Parallels gleichgezogen: Es gibt erstmals auch in der Virtualbox den Seamless-Modus. Er lässt Anwendungen auf dem Gast wie lokale Programme erscheinen, die direkt im Dock (unter Windows und Linux in der Taskleiste) auftauchen.

Virtualbox reicht den Prozessortyp direkt an das Gastsystem durch, sodass dieses eventuelle Optimierungen nutzen kann. Aktuell profitiert Virtualbox aber nicht von Mehrkernprozessoren: Der Gast bekommt immer nur einen einzigen Kern zugewiesen. Mehrere parallele Maschinen profitieren hingegen von der zusätzlichen Performance. Man sollte allerdings ausreichend Arbeitsspeicher einplanen: Schließlich laufen zwei vollständige Betriebssysteme parallel, da sollte mindestens 1 GByte Speicher vorhanden sein. Möchte man mehr als zwei virtuelle Maschinen mit Windows, Linux oder Mac OS X als Host oder Gast, kann Großzügigkeit nicht schaden. Im Test kam Windows XP als Gast mit 512 MByte Hauptspeicher gut zurecht: Das System fährt in 24 Sekunden hoch und ist unter Virtualbox somit 3 Sekunden schneller als mit Parallels' Desktop 3.0 for Mac.

Mehr Komfort für den Client bieten die Guest Additions: Installiert der Admin die Softwarepakete auf dem Gast, verbessert sich das Zusammenspiel mit dem Host. Unter Windows 2000 und XP sowie Linux-Distributionen klappt das ohne Weiteres – mit Windows Vista hakelt es, denn der Installer bricht mit einer Fehlermeldung ab. Die Gasterweiterungen lassen sich direkt über das Menü in die aktive virtuelle Maschine installieren. Hat man das Gastsystem neu gestartet, lässt sich zum Beispiel die Bildschirmauflösung weiter erhöhen. Im Test fiel auf, dass das Gastsystem außerdem etwa 2 % weniger Prozessorlast erzeugt.

Zur Sonne, zur Freiheit

Für Opensolaris auf x86-Maschinen steht auf der Projekthomepage eine erste Beta-Version zum Download bereit. Die Installation ist denkbar einfach. Man benötigt allerdings die zum Betriebssystem passende Version: x86 für 32-Bit-Hosts, amd64 für 64-Bitter. Nach der Installation mit *pkgadd* muss der Nutzer mit dem Kommando

```
export LD_LIBRARY_PATH=/opt/VirtualBox:↵
/opt/VirtualBox/qtgcc/lib:$LD_LIBRARY_PATH
```

den Suchpfad für die benötigten Bibliotheken ergänzen. Anschließend startet */opt/VirtualBox/VirtualBox* den Virtualisierer. Standardmäßig speichert Virtualbox alle virtuellen Maschinen und Festplatten-Images im Verzeichnis *~/.VirtualBox*. Sollte der Platz dort knapp werden, muss man einzelne VDI-Dateien an einen anderen Ort verlegen – der Ordner selbst lässt sich nicht verschieben.

In allen anderen Bereichen funktioniert Virtualbox auf Opensolaris wie unter Mac OS X: Die auf Opensolaris Developer Preview 2 getestete Version Beta 1 läuft weitgehend stabil – lediglich beim Einbinden von ISO-Images stürzte das Programm im Test einige Male ab. Opensolaris kann auch als Gast dienen: Zwar gibt es nur die Option „Solaris", Virtualbox kommt jedoch mit der offenen Variante ebenso zurecht.

Fazit

Mit Virtualbox ist eine leistungsfähige Virtualisierungsplattform in den Besitz von Sun übergegangen, in der Kategorie Plattform-Virtualisierer die einzige vollständige kostenlose und quelloffene Lösung. Man darf gespannt sein, wie Sun Virtualbox in seine Produktpalette integriert. Spannend bleibt außerdem, wie die Entwicklung für Mac OS X weitergeht, denn Virtualbox muss sich neben VMwares Fusion und Parallels' Desktop for Mac behaupten. (mr)

MARKUS FRANZ

ist Mitgründer und CTO der BF Blogform Search GmbH, Berlin. Er studiert Wirtschaftsinformatik an der Friedrich-Schiller-Universität in Jena.

Literatur

[1] Fred Hantelmann; Virtualisierung; Halböffentlich; Die quelloffene Virtualbox OSE; *iX* 5/07, S. 92

[2] Fred Hantelmann; Virtualisierung; Ins Glas geschaut; Marktübersicht: Server-Virtualisierung; *iX* 6/07, S. 104


ix0805086

iX-Wertung

⊕ großer Umfang an unterstützten Gastsystemen

⊕ Wandler für VMware-VMs

⊖ volle USB-Unterstützung und Remote Desktop nur in kommerzieller Version

Onlinequellen

Virtualbox	www.virtualbox.org
Hersteller	www.innotek.de
neuer Eigner	www.sun.com
virtuelle Maschinen	www.vmware.com/appliances/

Neuer Anlauf für Log-strukturierte Filesysteme

Rundkurs

Udo Seidel

Effizienteres Schreiben und Snapshots als kostenlose Zugabe versprechen Log-strukturierte Dateisysteme wie die im Februar 2008 freigegebene Version 2 von NILFS. Im *iX*-Labor musste eine Vorversion zeigen, ob sie Wort halten kann.

Verlässlichkeit, Performance, Skalierbarkeit und schnelle Wiederherstellung im Fehlerfall sind die Kriterien für ein gutes Dateisystem. Unter Linux greift der Admin auf ext3fs, XFS oder ReiserFS zurück – in geclusterten Umgebungen fällt die Wahl auf GFS oder OCFS2. Mit NILFS2 (New Implementation of a Log-structured File System) existiert seit einiger Zeit ein weiterer Kandidat, der den genannten Ansprüchen genügen will.

Log-strukturierte Dateisysteme (LFS) gehen zurück auf eine Idee von John Ousterhout – auch bekannt als Erfinder von Tcl/Tk – und Fred Douglis [1]. Sie basiert auf der Annahme, dass moderne Rechner über ausreichend Hauptspeicher verfügen, der es erlaubt, Lesezugriffe auf den Datenträger überwiegend aus dem Cache zu bedienen. Das eröffnet neue Wege, performantes Schreiben zu realisieren.

LFS behandeln den Datenträger wie ein „append-only log“ (siehe Kasten „Schreiben im Vorwärtsgang“). Der offensichtliche Gewinn besteht darin, dass Schreibzugriffe auf die Festplatte nur ein Minimum an Kopfbewegungen erfordern. Zudem ergibt sich automatisch die Möglichkeit, auf ältere Versionen der Datenbestände zuzugreifen (snapshotting). Da die reale Speicherkapazität begrenzt ist, muss jedoch ein Säuberungsprozess (garbage collector) nicht mehr benötigten Speicherplatz wieder freigeben.

Die erste Implementierung eines LFS verwirklichte die Forschungsgruppe um Ousterhout 1992 in Sprite, einem für Forschungszwecke entwickelten Betriebssystem. In die freien Unix-Varianten FreeBSD, OpenBSD und NetBSD hielt LFS ebenfalls Einzug. Es konnte sich dort aber nicht durchsetzen. Mit dem WAFL-Dateisystem (Write Anywhere File Layout) von Network Appliance existiert ein kommerzielles Produkt, das ebenfalls auf der Idee eines Log-strukturierten Dateisystems basiert. Für Linux gab es bereits mehrere Anläufe. Ein recht aktives Projekt ist NILFS beziehungsweise die verbesserte Version NILFS2.

Datenträger portioniert

Abbildung 1 zeigt das Layout einer NILFS2-Partition. Erwartungsgemäß enthält der Superblock die Parameter des Dateisystems, beispielsweise die Blockgröße und den Mount-Zähler. Ähnlich wie die „klassischen“ Dateisysteme verwaltet NILFS2 den Plattenplatz nicht als ein großes Paket. Die Unterteilung in sogenannte Segmente (full segments) erhöht die Effizienz des Garbage Collectors. Die Anzahl der Blöcke pro Segment hängt von der Größe des Datenspeichers ab – das Minimum ist 16. Schreibzugriffe fasst NILFS2 zu logischen Segmenten zusammen, die wiederum aus partiellen Segmenten bestehen (siehe Abbildung 1). Letztere enthalten mindestens zwei Blöcke.

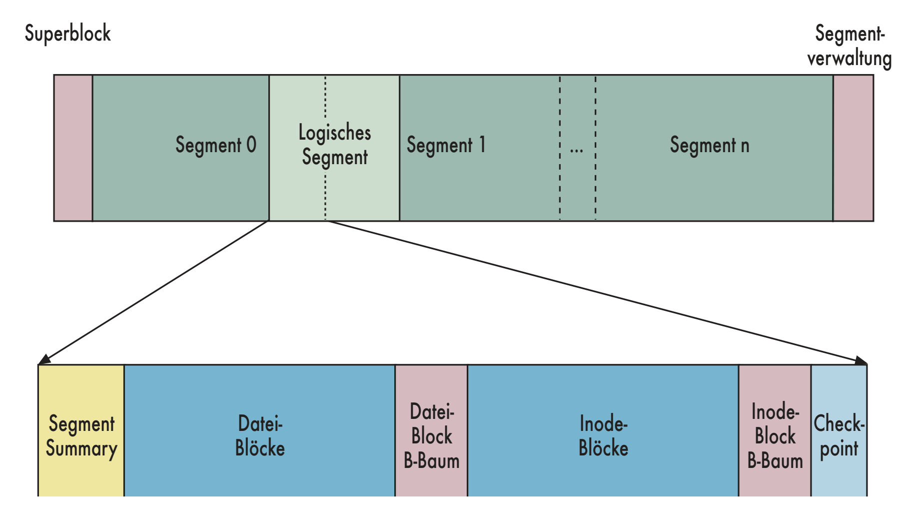
Für die Übersetzung von Datei-Blockadressen und Inode-Nummern in Datenträger-Blockadressen (file/inode block mapping) verwendet NILFS2 je zwei B-Bäume pro partiellem Segment. Den Aufbau der Verzeichnisse hat das Dateisystem von ext2fs geerbt. Ebenso die damit verbundenen Nachteile, etwa die Längenbegrenzung für Dateinamen und mangelnde Performance bei Operationen in großen Verzeichnissen. Später wollen die Entwickler Verzeichnisse ebenfalls als B-Bäume implementieren.

Jedes partielle Segment enthält am Anfang eine sogenannte Segment Summary, die unter anderem Auskunft über seine Größe und die Nutzung der einzelnen Blöcke gibt. Darauf folgt der Datenbereich, der sowohl Datenblöcke als auch Inodes nebst den zugehörigen B-Bäumen enthält. Am Ende befindet sich ein Checkpoint-Bereich.

Während die Segment Summary hauptsächlich für den Garbage Collector und *fsck* wichtig ist, enthält der Checkpoint Informationen für Lese- und Schreibzugriffe. Insbesondere befindet sich dort ein Verweis auf den ersten Block – die „Wurzel“ – des Inode-B-Baums. Mit dem Schreiben der Information in den Checkpoint-Bereich geht das Dateisystem von einem konsistenten Zustand in den nächsten über.

Markante Punkte

Designbedingt entspricht ein Checkpoint bei NILFS2 bereits einem Snapshot – einem konsistenten Dateisystemzustand zu einem bestimmten Zeitpunkt. Konsequenterweise lassen sich Checkpoints in Snapshots überführen und umgekehrt. Aus administrativer Sicht unterscheiden sie sich dadurch, dass Snapshots per *mount*-Befehl zugänglich sind und bei der routinemäßigen Garbage Collection erhalten bleiben.



Stückweise: NILFS2 teilt den Datenträger in Segmente ein (Abb. 1).

Wer mit NILFS2 experimentieren will, muss zunächst den Quellcode von der Projekt-Homepage (www.nilfs.org) herunterladen und übersetzen – fertig kompilierte Pakete gibt es nicht. Zum Übersetzen benötigt man außerdem den Quellcode des installierten Kernels (Version 2.6.11 oder neuer). Die Software gliedert sich in zwei Teile: das Kernel-Modul *nilfs2.ko* und die dazugehörigen Werkzeuge. Zu Letzteren gehören die Hilfsprogramme *mkfs.nilfs2* und *mount.nilfs2* zum Anlegen und Mounten des Dateisystems, der Garbage Collector *nilfs_cleanerd* sowie die Tools zur Checkpoint- und Snapshot-Verwaltung. Im Test kam die im Dezember 2007 erschienene Version 2.0.0-testing8 zum Einsatz.

Nach dem Laden des Kernel-Moduls lässt sich die mit *mkfs.nilfs2* formatierte Partition mit *mount –t nilfs2* einhängen. Dabei startet automatisch der Garbage Collector – es sei denn, der Administrator hängt das Dateisystem nur zum Lesen ein. Das *umount*-Kommando beendet *nilfs_cleanerd* wieder.

In der Datei */etc/nilfs_cleanerd.conf* lassen sich die Betriebsparameter des Cleaners einstellen. Momentan ist nur eine „Säuberungsrichtlinie“ verfügbar: das Löschen der Checkpoints in chronologischer Reihenfolge, beginnend mit dem ältesten. Weiterhin kann der Admin in der Datei festlegen, wie lange die Segmente eines Checkpoints unangetastet bleiben (*protection_period*) und wie viele Segmente er auf einmal löschen soll (*nsegments_per_clean*). Voreingestellt sind 3600 Sekunden und 2 Segmente. Das bedeutet, dass der Speicherplatz, den eine gelöschte Datei zuvor belegt hat, erst nach etwa einer Stunde wieder zur Verfügung steht. Beim Tuning gilt es, einen Kompromiss zwischen der Verfügbarkeit von Dateisystemzuständen aus der Vergangenheit und dem benötigten Speicherplatz zu finden.

In der gegenwärtigen Implementierung verwendet NILFS2 pro eingehängtem Dateisystem einen Garbage-Collector-Prozess. Ein separates Tunen des *nilfs_cleanerd* ist deshalb nur bedingt möglich. Der Admin muss den automatisch gestarteten Prozess beenden und manuell unter Angabe der gewünschten Konfigurationsdatei neu starten. Ein Wrapper-Skript für das *mount*-Kommando mit geschickt gewählter Namenskonvention für die Konfigurationsdatei hilft dabei, befindet sich aber leider nicht im Lieferumfang von NILFS2. Hier haben die Entwickler noch ein Stück Arbeit vor sich.

Das Checkpoint- und Snapshot-Management von NILFS2 ist zwar noch nicht so elegant wie das von Netapps WAFL, aber durchaus nutzbar. Mit den Kommandozeilen-Tools kann der Admin Checkpoints und Snapshots anzeigen lassen (*lscp*), anlegen (*mkcp*), ineinander überführen (*chcp*) und löschen (*rmcp*). Das Anlegen von reinen Checkpoints ist normalerweise nicht nötig, da NILFS2 es spätestens 5 Sekunden nach dem letzten Schreiben selbst erledigt.

Schreiben im Vorwärtsgang

Die Besonderheit von Log-strukturierten Dateisystemen ist die Art des Schreibvorgangs. Abbildung 2 zeigt ein beispielhaftes Szenario bei NILFS2: In einem Verzeichnis befindet sich zunächst die Datei *A* mit den zwei Blöcken *A1* und *A2* (oben). Sowohl Daten- als auch Inode-Blöcke für das Verzeichnis samt Inhalt befinden sich im partiellen Segment *n*. In seinem Checkpoint-Bereich steht ein Verweis auf den ersten Block des Inode-B-Baums und damit indirekt auf die Inodes.

Legt der Nutzer danach eine Datei *B* an, platziert NILFS2 sie in einem zweiten partiellen Segment *n+1* und aktualisiert den Inode-Bereich so, dass er beide Dateien beinhaltet. Anschließend legt es einen neuen Checkpoint an (Mitte).

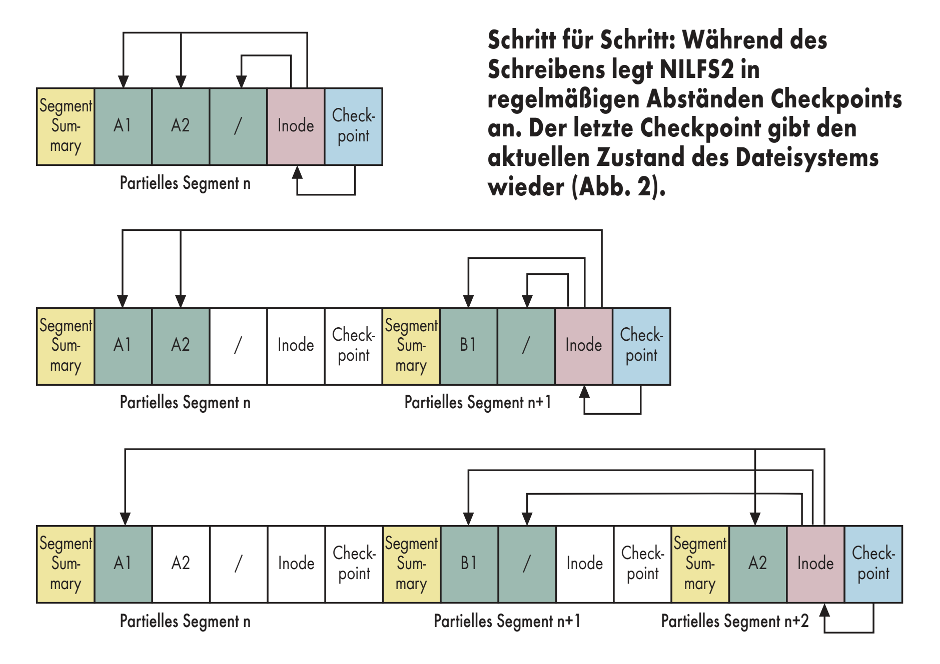
Ändert sich der Inhalt von *A*, kopiert das Dateisystem die Inode und die betroffenen Blöcke in ein weiteres partielles Segment, führt dort die Änderungen durch und erzeugt einen weiteren Checkpoint (unten). Alle älteren Checkpoints, die die früheren Versionen enthalten, bleiben bestehen, bis der Garbage Collector sie entfernt.

Reise in die Vergangenheit

Will der Administrator auf den Datenzustand eines bestimmten Zeitpunktes zugreifen, muss ein Snapshot anstelle eines Checkpoints vorhanden sein. Das Kommando *mkcp –s* legt einen Snapshot zum gegenwärtigen Zeitpunkt an, *chcp ss <nummer>* wandelt einen Checkpoint in einen Snapshot um. Überflüssige Snapshots kann der Admin wieder in Checkpoints konvertieren. Wer nicht warten will, bis *nilfs_cleanerd* einen Checkpoint beseitigt, kann ihn mit *rmcp <nummer>* manuell löschen. Dabei ist allerdings zu beachten, dass manuelles Löschen nicht den belegten Speicherplatz freigibt – das erledigt zu gegebener Zeit der Cleaner-Daemon.

Für Zugriffe auf einen Snapshot muss man dessen Nummer beim Mounten mit der Option *–o cp=<nummer>* angeben. NILFS2 erlaubt es nicht, einen Snapshot im Schreibmodus zu mounten. Das ist jedoch kein Manko, da so etwas der Idee eines LFS widerspricht.

Im Vergleich mit ext3fs lässt die Performance von NILFS2 noch zu wünschen übrig. Selbst beim sequentiellen Schreiben – die Spezialität eines LFS – bleibt NILFS2 je nach verwendeter Hardware mehr oder weniger deutlich hinter seinem Konkurrenten zurück. Auch in den übrigen Teildisziplinen des *bonnie++* schlägt sich der Neuling meist schlechter als das Linux-Urgestein. Lediglich beim Löschen von Dateien hat NILFS2 die Nase weit vorn. Bedenkt man jedoch, dass die Arbeit des Garbage Collectors nicht in die gemessene Zeit eingeht, ist das beileibe kein Kunststück.



Schritt für Schritt: Während des Schreibens legt NILFS2 in regelmäßigen Abständen Checkpoints an. Der letzte Checkpoint gibt den aktuellen Zustand des Dateisystems wieder (Abb. 2).

Tests mit NILFS2 als Samba-Share zeigten keine Auffälligkeiten. Sowohl das Live-Dateisystem als auch die Snapshots ließen sich ohne Schwierigkeiten exportieren. Die fehlende Unterstützung für ACLs schränkt die Anwendungsmöglichkeiten allerdings ein.

NFS-Freigaben ließen sich bei früheren Versionen nicht mounten. Mittlerweile kann man Verzeichnisse auf einer NILFS2-Partition gar nicht mehr per NFS exportieren. Für einen Fileserver oder ein NAS-System ist das Dateisystem daher nicht geeignet.

Fazit

NILFS2 ist ein vielversprechender Ansatz für ein LFS unter Linux. Die durchgeführten Tests zeigen aber, dass es sich für den Einsatz in Produktionsumgebungen noch nicht eignet. Auch die Performance lässt noch etwas zu wünschen übrig. Immerhin stehen jedoch wichtige Punkte wie ein verbesserter Garbage Collector, das Snapshot-Management oder ACL-Unterstützung bereits auf der To-do-Liste der Entwickler. (mr)

DR. UDO SEIDEL

leitet eine Unix/Linux-Sysadmin-Gruppe bei der Amadeus Data Processing GmbH in Erding.

Literatur

[1] John Ousterhout, Fred Douglis; Beating the I/O Bottleneck: A Case for Log-Structured File Systems; ftp://ftp.cs.berkeley.edu/ucb/sprite/papers/lfs-case.ps



Blacklist-Nutzung zeigt Internet-Missbrauch in Echtzeit

Ausgefragt

Sebastian Ganschow, Christian J. Dietrich, Norbert Pohlmann

Anti-Spam-Blacklists erhalten zum Teil viele Tausend DNS-Abfragen pro Sekunde, die sich direkt auf den weltweiten E-Mail-Verkehr beziehen. Betreiber von DNSBL-Servern haben damit einen guten Blick auf das Geschehen – müssen dafür aber regelrechte Datengebirge bezwingen.

IP-Blacklisting ist ein wichtiger Schutzmechanismus im Kampf gegen Internet-Missbrauch, vor allem Spam. Eine Reihe von Blacklists lässt sich kostenlos über das Internet nutzen. Üblicherweise kommt das DNS-Protokoll für deren Abfrage zum Einsatz (DNSBL). Außer dem eigentlichen Inhalt der Blacklists, also den Spam-Quellen in Form von IP-Adressen, sind auch die Abfragen ein interessantes Analyseobjekt – sowohl die abfragenden Hosts als auch die abgefragten Adressen betreffend.

Wer Zugriff auf die Abfragedaten hat, kann unter anderem den Anteil des Inhalts einer Blacklist bestimmen, der überhaupt abgefragt wird. Darüber hinaus kann man die Menge an positiven Antworten, also Treffern auf der Blacklist, ins Verhältnis setzen zu allen Anfragen („Trefferquote“ oder „Hit Rate“). Ferner lässt sich bestimmen, wie sich etwa das Spam-Aufkommen entwickelt oder welche Nutzerzahl die Blacklist hat – allesamt wichtige Eckdaten für Wirksamkeitsbetrachtungen und Optimierungen.

In einem Zeitraum von fast einem halben Jahr wurden die Anfragen an zwei öffentliche Blacklists untersucht, darunter die vom Projekt „NiX Spam“ der *iX*. Sie umfasste zu Beginn der Untersuchung im Juli 2007 etwa 78 000 IP-Adressen aus 166 Ländern, zum Ende (Januar 2008) bereits über 400 000 Adressen. Zum Vergleich diente die „Blackholes“-Liste (www.five-ten-sg.com). Für beide betreiben die Autoren DNS-Slave-Server, sodass sie einen repräsentativen Ausschnitt aus den Anfragen an die Blacklists „mitschneiden“ können.

Sklavenbetreiber lesen mit

Die NiX-Spam-Liste verfügte am Ende des Erfassungszeitraums über zehn DNS-Server, von denen zwei während der Messungen hinzukamen. Mit jedem hinzukommenden Server sollte die Anzahl der Anfragen pro Server zumindest vorübergehend abnehmen. Die Anzahl der Anfragen stieg jedoch praktisch über den gesamten Messzeitraum hinweg unbeirrt: Zu Beginn lag die Zahl der Requests pro Tag bei rund 5,5 Mio. Zuletzt liefen täglich etwa 9,5 Mio. Anfragen auf. Die Trendlinie deutet an, dass von einem weiteren Anstieg auszugehen ist.

Während die abgefragten IP-Adressen zeigen, wo Spam und erwünschte E-Mails herkommen, enthalten die Adressen der Abfragenden selbst Hinweise darauf, wer die Nutzer der Blacklist sind. Bei NiX Spam sind es pro Tag etwa 10 000 verschiedene Adressen und damit schätzungsweise mindestens ebenso viele Mailserver-Betreiber. Da die vorliegende Messung lediglich an einem Server stattfand, blieben eventuelle weitere Anwender der anderen Server unberücksichtigt. Da die DNS-Anfragen jedoch per Round Robin praktisch gleichmäßig an alle Server gehen, dürfte das Ergebnis dennoch realistisch sein.

DNS-Resolver können ferner Antworten zwischenspeichern, sodass vermutlich nicht alle Anfragen tatsächlich bis zum Server der Blacklist durchdringen. Unter Vernachlässigung des Resolver-Caching entspricht jede Anfrage an die Blacklist einer SMTP-Session (zumeist mit einer empfangenen oder abgewiesenen E-Mail). Interessanterweise blieb die Anzahl der anfragenden IP-Adressen über den gesamten Messzeitraum hinweg relativ konstant, während die Zahl der Anfragen deutlich wuchs. Eine mögliche Erklärung dafür ist ein Anstieg des gesamten E-Mail-Volumens.

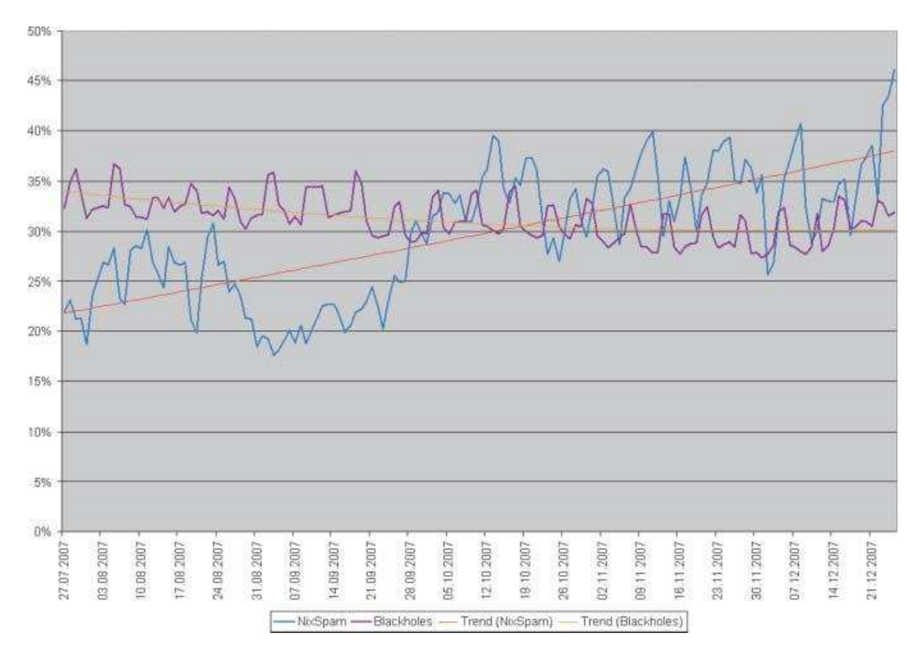
Befindet sich eine abgefragte IP-Adresse auf der Blacklist, gibt der DNSBL-Server eine positive Antwort. Die Zahl verschiedener IP-Adressen

gibt Aufschluss über die Menge mailsendender Hosts. Da Spam über 90 Prozent aller Mails ausmacht, tauchen vor allem solche IP-Adressen auf, die den Spam-Versendern zur Verfügung stehen. Die Abfragen an den NiX-Spam-Slave beziehen sich durchschnittlich auf 1,2 Mio. Adressen täglich. Da manche davon mehrmals auftauchen, sind es insgesamt deutlich mehr Abfragen.

Am 24. Dezember 2007 etwa fragten NiX-Spam-Anwender exakt 1 158 148 verschiedene IP-Adressen ab. Davon standen nur rund 10 % (112 980) auf der Blacklist. Die Liste umfasste damals rund 300 000 IP-Adressen. Nur gut ein Drittel der gelisteten IP-Adressen wurde also an diesem Tag überhaupt abgefragt. Einige Monate zuvor, am 1. August 2007, wurden „nur“ 781 472 verschiedene IP-Adressen im Laufe des Tages abgefragt. Die Zahl verseuchter, für den Spam-Versand missbrauchter Systeme steigt anscheinend nach wie vor.

Blackholes als Vergleichsbasis

Die zum Vergleich herangezogene Blackholes-Liste verfügte im Untersuchungszeitraum konstant über 14 DNS-Server. Anders als bei „NiX Spam“ zeigt der Trend der Anfragen abwärts. Zugleich hat sich die Zahl der anfragenden IP-Adressen erhöht. Zwischen der Anzahl der abgefragten IP-Adressen und der positiven Antworten gibt es – unerklärlicherweise – kaum Abweichungen.



Die NiX-Spam-Liste nimmt laufend neue Spam-Fallen in Betrieb und steigert dadurch den Anteil positiver Antworten (Abb. 1).

Bei Blackholes liegt die Zahl der abgefragten unterschiedlichen IP-Adressen pro Tag im Durchschnitt bei rund 1 Mio. Am 24. Dezember 2007 standen davon etwa 320 000 auf der Liste. Dies entspricht rund 32 %, mehr als dreimal so viel wie bei NiX Spam. Über den gesamten Dezember 2007 hinweg belief sich die Anzahl an verschiedenen IP-Adressen auf 4 744 440, während der gesamten fünf Monate zeigten sich sogar 17 742 550 – offenbar vor allem aus Bereichen dynamisch immer wieder neu vergebener Adressen.

Anfang August belief sich die Anzahl an verschiedenen, abgefragten IP-Adressen der Blackholes auf 1 006 668. Hiervon standen etwa 228 000 auf der Blacklist, die sich damit potenziell spammenden Hosts zuordnen ließen.

Trefferquote ist nicht alles

Ein wichtiger Indikator dafür, ob sich das Abfragen einer Blacklist überhaupt lohnt, ist der Anteil der positiv beantworteten Anfragen. Je höher die Trefferwahrscheinlichkeit, desto mehr Spam-Nachrichten könnten mithilfe der Blacklist erkannt werden und desto effektiver ist die Liste. Andererseits ist die „Hit Rate“ in Verbindung mit der Gesamtanzahl an Anfragen auch ein Indiz für die Menge an Spam, die versendet wird.

Der Trefferanteil bei NiX Spam stieg über den gesamten Zeitraum der Untersuchung hinweg deutlich (Abb. 1). Er hat sich während des Zeitraums fast verdoppelt und lag zuletzt bei weit über 40 %. Eine hohe Hit Rate bedeutet in erster Linie, dass viele abgefragte Adressen tatsächlich auf der Liste stehen. Dies geht allerdings nur so lange gut, wie die Zahl der fehlerhaft gelisteten IP-Adressen (False Positives) sehr gering bleibt. Für die Bewertung der Qualität einer Blacklist muss daher

iX-TRACT

- Die bei Anti-Spam-Blacklists abgefragten IP-Adressen sind mindestens ebenso interessant wie der eigentliche Datenbestand, da sie ein realistisches Bild vom laufenden E-Mail-Geschehen vermitteln.
- Die Abfragen bei Blacklists geben sowohl die räumliche Verteilung von Spam-Quellen als auch den zeitlichen Ablauf von Spam-Angriffen wieder.
- Spam-Versender nutzen laufend über eine Million IP-Adressen, meist über verseuchte PCs. Sie verwenden einen Großteil davon nur für äußerst kurze Zeit.

neben der Trefferquote immer auch der False-Positive-Anteil berücksichtigt werden. Eine automatische Messung der False-Positive-Rate gestaltet sich jedoch mindestens so schwierig wie die Definition von „False Positive“ an sich und ist derzeit Gegenstand der Forschung.

Das Sinken der Zugriffszahlen auf die Blackholes könnte auf deren relativ hohe False-Positive-Rate zurückzuführen sein. Al Iverson hat etwa zum gleichen Zeitpunkt, zu dem unsere Messungen begannen, angefangen, verschiedene Blacklists zu analysieren und die Blackholes schlecht bewertet (www.dnsbl.com).

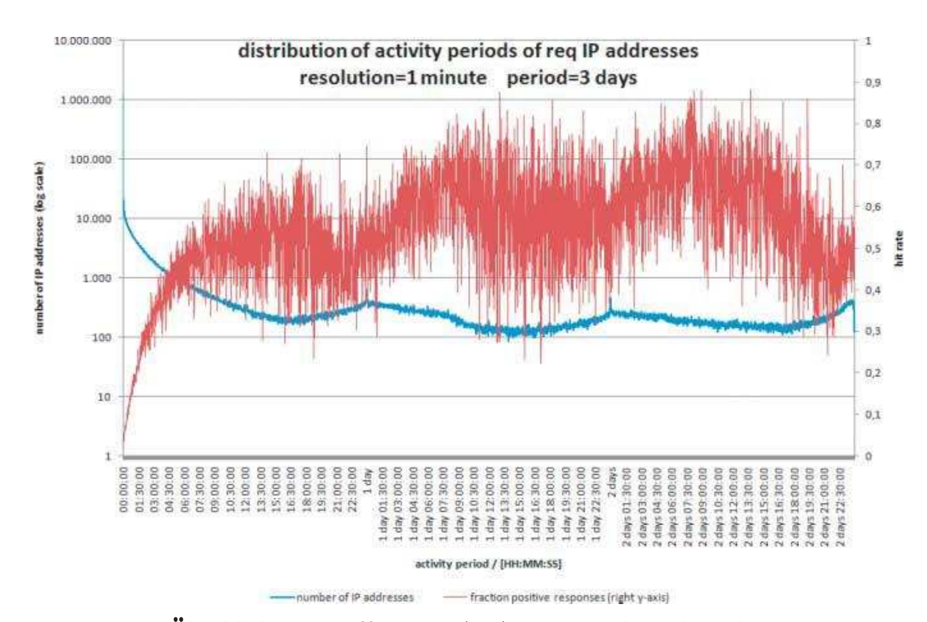
Bei einem Spam-Anteil von zurzeit über 90 % treffen sämtliche Statistiken zwangsläufig vor allem Aussagen über unerwünschte E-Mails – so auch diejenige über Quellregionen (siehe Tabellen). Bei beiden Blacklists belegen die USA und Russland die ersten beiden Plätze. Neun Länder finden sich in den „Top 10“ beider Blacklists. Ein Drittel der Anfragen für IP-Adressen aus den USA beantwortet NiX Spam positiv. Bei den IP-Adressen aus Russland ist es sogar die Hälfte der Anfragen. Der Anteil für aus Deutschland empfangene Spam-Mails liegt nur bei 10 %. Daraus lässt sich schließen, dass die Nutzer dieser Blacklist größtenteils Spam aus den USA, Russland und Korea empfangen.

Der Anteil positiv beantworteter Anfragen liegt bei Blackholes wesentlich niedriger. Auf Anfragen für IP-Adressen aus den USA liefert sie nur in rund einem Viertel der Fälle eine positive Antwort. Immerhin ein Drittel der Anfragen zu deutschen IP-Adressen beantwortet sie jedoch positiv (NiX Spam: 10 %).

E-Mails aus China sind offenbar meist Spam. Das Ergebnis deckt sich mit den Aussagen von Anti-Spam-Dienstleistern. In absoluten Zahlen werden die AS von den türkischen, italienischen und polnischen Telecoms (TTnet, Telecom Italia und TP) hier am häufigsten abgefragt.

Unter den bei Blackholes abgefragten Adressen fallen die AS von Arcor und Korea Telecom aus dem Rahmen, denn der Anteil an positiven Antworten ist dort mit jeweils fast 99 % sehr hoch. Fast jede IP-Adresse, zu der die Blackholes-Liste konsultiert wurde, stand auch tatsächlich auf der Blacklist. Man könnte aufgrund dieses Ergebnisses auf gewisse Abneigungen des Blacklist-Betreibers schließen. Die zweite Reihe bilden die beiden autonomen Systeme von Chinanet (AS 4837 und 4134). Der relative Anteil an positiv beantworteten Anfragen liegt in beiden Fällen bei rund 87 %. Sie verursachen ein deutlich höheres absolutes Aufkommen an Anfragen als Arcor und Korea Telecom.

Auf der NiX-Spam-Liste spielt Arcor dagegen keine große Rolle. Die abgefragten Adressen werden dort derzeit dominiert von der Koreanischen Telecom (11 Mio. Abfragen, 80 % davon positiv beantwortet), TTnet (10 Mio./44 %) und Telefonica del Peru (5 Mio./51 %). Die Deutsche Telekom taucht, was die Abfragen angeht, mit 3,2 Mio. pro Tag erst auf Platz 10 auf, und davon werden nur 730 000 (23 %) positiv beantwortet, ein besonders geringer Wert.



Drei Tage im Überblick: Die Trefferquote (rot) steigt mit der Lebensdauer eines Eintrags, doch die meisten Einträge sind nur für extrem kurze Zeit aktiv (Abb. 2).

Sehr geringe Lebensdauer

Bei NiX Spam gelistete IP-Adressen fallen nach drei Tagen wieder aus der Blacklist, wenn von ihnen nicht erneut Spam ausgeht. Bisher basierte dieser Wert allein auf Experimenten. Eine Statistik über die Verteilung der Zeiträume, in denen IP-Adressen abgefragt werden, zeigt, dass tatsächlich nur rund 8 % der abgefragten IP-Adressen überhaupt über einen Zeitraum von mehr als drei Tagen auftauchen – sprich: E-Mails (meist Spam) versenden. Anders ausgedrückt: 92 % aller abgefragten IP-Adressen werden in einem Zeitraum von drei Tagen abgefragt. Drei von vier abgefragten IP-Adressen scheinen sogar nur maximal einen Tag lang aktiv zu sein.

Noch deutlicher zeigt sich dieses Phänomen hinsichtlich der Aktivitätszeiträume innerhalb eines Tages (Abb. 2). Die x-Achse stellt den Aktivitätszeitraum, die y-Achse die Anzahl abgefragter IP-Adressen in logarithmischer Skalierung dar. Wird eine IP-Adresse beispielsweise je einmal um 12:00 und um 13:00 Uhr (und dann im Messzeitraum nicht mehr) abgefragt, gilt sie als eine Stunde lang aktiv.

NiX-Spam-Abfragen nach Ländern

Land	Anfragen	positive Antworten
USA	36 687 286	11 750 439
Russland	15 070 834	8 406 100
Deutschland	14 957 047	1 494 028
Südkorea	14 067 659	8 604 614
Brasilien	8 592 407	2 611 582
Großbritannien	8 200 419	2 454 146
Polen	8 049 853	2 796 431
Türkei	7 747 089	2 016 771
Spanien	6 848 259	2 371 162
Italien	6 695 144	1 682 333

Top 10 der bei der NiX-Spam-Blacklist abgefragten IP-Adressen nach Ländern

Blackholes-Abfragen nach Ländern

Land	Anfragen	positive Antworten
USA	19 700 000	4 760 000
Russland	6 325 000	1 122 000
Türkei	4 441 000	1 573 000
Deutschland	4 035 000	1 368 000
Brasilien	3 852 000	1 194 000
Italien	3 778 000	1 135 000
Großbritannien	3 253 000	1 289 000
Polen	3 226 000	1 542 000
China	3 109 000	2 729 000
Spanien	2 774 000	915 000

Top 10 der abgefragten IP-Adressen bei Blackholes nach Ländern

Die Darstellung verdeutlicht, dass ein großer Teil der Anfragen eine sehr kurze Aktivität aufweist. Von den pro Tag rund 1,35 Mio. verschiedenen, abgefragten IP-Adressen sind rund 496 000 IP-Adressen (entsprechen 37 %) weniger als eine Minute lang aktiv. In fast 93 % der Fälle tauchen diese Adressen auch tatsächlich nur ein einziges Mal innerhalb eines Tages auf. Weitere 6 % der „kurzlebigen“ Adressen tauchen innerhalb der ersten Minute zweimal auf. Ein lokales Maximum befindet sich zwischen 23 und 24 Stunden, offenbar durch dauerhaft betriebene Mailserver verursacht. Während eines längeren Zeitraums, etwa über drei Tage, zeigt sich ein weiteres Muster.

Die Erkennungsrate fällt erwartungsgemäß bei sehr kurzlebigen IP-Adressen entsprechend gering aus. Da eine IP-Adresse zunächst als Spam-Quelle auffallen und in die Blacklist gelangen muss, haben kurzlebige oder einmal verwendete IP-Adressen gute Chancen, nicht erkannt zu werden. Für Betreiber von Blacklists bedeutet das Ergebnis jedoch die Herausforderung, die Trägheit der Systeme zu minimieren. Keine leichte Aufgabe, wenn man nicht riskieren möchte, zu viele Adressen fälschlicherweise zu blockieren.

Ein ebenfalls zu beobachtendes, noch unklares Phänomen sind „selbstabfragende“ IP-Adressen: Gelegentlich entspricht die abgefragte IP-Adresse der abfragenden. Das fand während des Messzeitraums über 150 000-mal statt, etwas zu häufig etwa für gelegentliche Experimente von Endanwendern. Eventuell gehen solche selbstbezüglichen Abfragen von Bots aus, die prüfen, ob ihr Wirt bereits unangenehm aufgefallen ist – oder von unvorsichtig konfigurierten Mailservern.

Fazit und Ausblick

Die Verhaltensanalyse von Blacklists kann Licht in das Dunkel bringen, wenn es um ein Gefühl für die Nutzer einer Blacklist sowie Eigenschaften der gelisteten Adressen geht. Langfristig lassen sich möglicherweise aus dem Abfrageverhalten einer Blacklist Optimierungen wie zur Lebensdauer einer IP-Adresse auf der Blacklist ableiten. Derzeit stellt darüber hinaus die automatische Messung des False-Positive-Anteils einer Blacklist noch eine Forschungsaufgabe dar. (un)

SEBASTIAN GANSCHOW

arbeitet als Senior Network Engineer bei der Dr. Bülow & Masiak GmbH in Marl. Er unterstützt das Institut für Internet-Sicherheit an der FH Gelsenkirchen im Forschungsbereich E-Mail-Sicherheit.

CHRISTIAN DIETRICH

ist Mitarbeiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen und für den Forschungsbereich E-Mail-Sicherheit verantwortlich.

PROF. DR. NORBERT POHLMANN

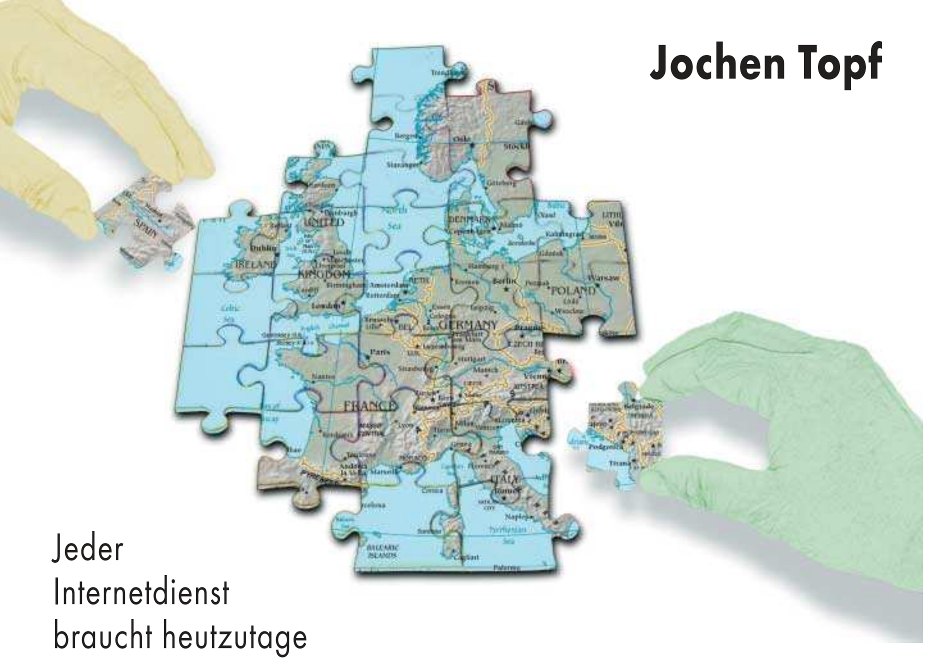
ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen.



Freies Landkartenprojekt: OpenStreetMap

Weltkarte zum Mitmachen

Jochen Topf



Jeder Internetdienst braucht heutzutage seine interaktive Karte, und jeden Tag gehen neue Karten-Mashups online. Aber diese Karten sind häufig nur vorgefertigte Bitmaps unter einer einschränkenden Lizenz und ohne Zugriff auf die Rohdaten. Abhilfe verspricht das Open-StreetMap-Projekt, das Geodaten der ganzen Welt sammelt.

Das Projekt „OpenStreetMap“ (OSM, siehe „Onlinequellen“ [a]) will eine freie Karte der ganzen Welt zusammenstellen. Dabei geht es in erster Linie um Straßendaten, hinzu kommen Fuß- und Waldwege, Eisenbahnen, Seen und Flüsse, Wald- und Industrieflächen und vieles andere vom Briefkasten bis zum Skilift.

Tausende von Hobbyisten sammeln die Daten, indem sie mit GPS-Geräten (Global Positioning System) durch die Gegend laufen oder fahren und sich dabei Straßennamen und andere Informationen notieren. Alternativ dienen Satelliten- oder Luftbilder als Ausgangspunkt. Um die Erkundung vor Ort kommt man aber nicht herum, da das Luftbild weder Straßennamen noch andere Details zeigt. Und diese einer bestehenden Karte zu entnehmen, ist lizenzrechtlich nicht erlaubt. Manchmal treffen sich Interessierte zu sogenannten „Mapping Parties“, bei denen sie meist ein Wochenende lang gemeinsam die Geodaten eines bestimmten Bereiches erfassen. Bei solchen Veranstaltungen geht es nicht nur um die Arbeit, sie dienen vor allem dem Kontakt mit Gleichgesinnten.

Flexibilität durch Tagging

OpenStreetMap ist ähnlich wie ein Wiki organisiert: Jeder kann nach der einfachen Anmeldung neue Daten eintragen und bestehende ändern. Da die Datenbank alle Versionen von Objekten speichert, lässt sich jeder historische Stand rekonstruieren, etwa um gelöschte Objekte wiederherzustellen.

Jedes geometrische Objekt verfügt über beliebige Attribute („Tags“). Das ermöglicht Flexibilität: Jeder kann die Dinge in die Datenbank eintragen, die ihn interessieren, ohne das vorher mit anderen absprechen zu müssen. Damit das nicht im Chaos endet, diskutieren die Teilnehmer Konventionen und Standards auf der Mailingliste und im Projekt-Wiki und dokumentieren sie. Für die üblichen Straßentypen und Dinge wie Briefkästen und Hotels gibt es schon passende Tags, an die sich die meisten Teilnehmer halten. Es bleibt aber jedem unbenommen, weitere Tags zu vergeben.

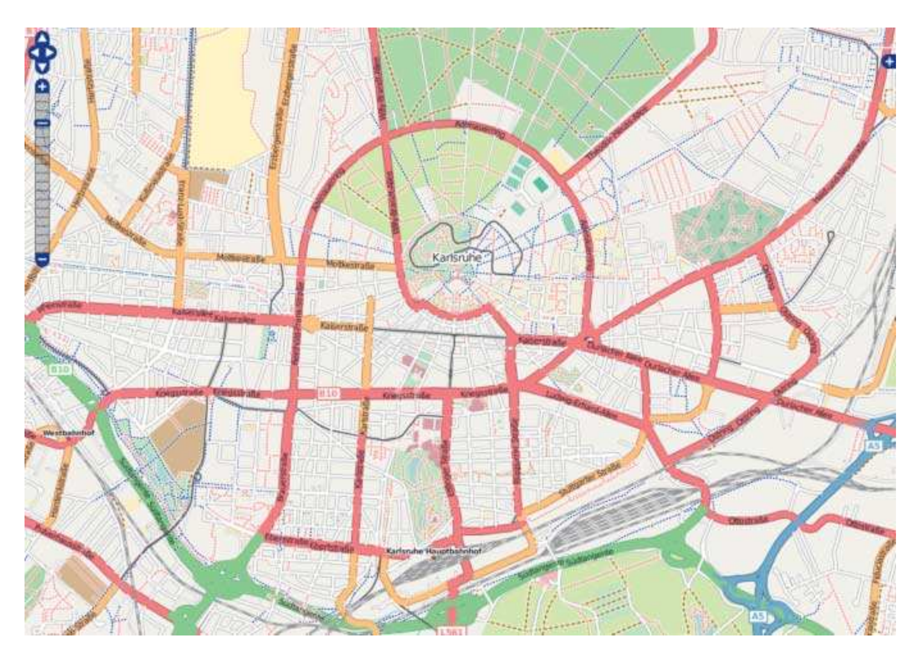
Jeder Einzelne entscheidet auch, welche Informationen er überhaupt beitragen kann und will. Unbekannte Daten, zum Beispiel die Geschwindigkeitsbeschränkung auf einer Straße, lässt man einfach weg. Es wird sich schon später jemand finden, der sie ergänzt.

Dieser offene und etwas hemdsärmelige Ansatz hat bereits viel Kritik einstecken müssen, aber das Ergebnis sieht durchaus vielversprechend aus. Die Datenqualität ist allerdings noch recht uneinheitlich. In manchen Regionen herrscht weitgehend Leere, andere sehen zwar besser aus, enthalten aber noch viele Fehler. Es gibt aber auch viele vollständige Ecken, deren Daten denen kommerzieller Karten das Wasser reichen können. Insbesondere bei Fuß-, Rad- und Waldwegen ist die Abdeckung der OSM-Karten häufig besser als die der üblichen Anbieter, die für den Autoverkehr optimieren.

Zwar herrscht noch viel Durcheinander und früher oder später wird es zu Vandalismus kommen, aber Wikipedia hat gezeigt, dass man solche Schwierigkeiten in den Griff bekommen kann, ohne die Freiheit zu stark einschränken zu müssen. Ein Streit zwischen türkischen und griechischen Zyprioten über die zu verwendenden Namen hat die zu erwartenden Konflikte demonstriert – Karten können eben auch ein Mittel der Politik sein.

Nachdem es nach der Gründung vor dreieinhalb Jahren in England langsam voranging, hat das Projekt im letzten Jahr einen großen Schritt nach vorne getan. Sein Schwerpunkt liegt in Europa, vor allem in Großbritannien und Deutschland ist die Abdeckung schon gut. Nach der ersten Mapping Party überhaupt auf der Isle of Wight im Mai 2006 war die Insel das erste systematisch und komplett erfasste Gebiet.

Im Frühsommer 2007 war Karlsruhe als erste deutsche Großstadt vollständig erfasst. Das vor einem Jahr noch leere



Karlsruhe war als erste deutsche Großstadt nahezu vollständig im OpenStreetMap-Projekt erfasst. In mancher Hinsicht sogar besser als anderswo: Die Daten enthalten nicht nur Straßen, sondern auch viele Fuß- und Waldwege (Abb. 1).

Berlin weist heute zumindest die inneren Stadtteile komplett auf. In ländlicheren Gebieten ist die Abdeckung allerdings meist noch etwas dünner. Auch außerhalb Europas geht es voran: So wurde Bagdad, von dem kaum Karten, aber gute Luftbilder zu bekommen sind, aus der Ferne in großen Teilen erfasst. Die Straßennamen und andere, nur vom Boden erkennbare Details, fehlen dort allerdings. Wer sich selbst ein Bild verschaffen will, schaue sich die Karte auf der Webseite des Projekts an oder vergleiche verschiedene Versionen der OSM-Karten mit Google-Karten [b].

Freie Daten aus den USA

Zusätzlich zu den speziell für OSM gesammelten Daten stehen inzwischen einige andere Quellen zur Verfügung: Die holländische Firma AND hat ihren gesamten professionell erfassten Datenbestand der Niederlande gespendet. Aus dem Frida-Projekt der Firma Intevation stammen die Geodaten für die Stadt Osnabrück. Und im Februar kamen die sogenannten TIGER-Daten hinzu, die die US-amerikanische Behörde für Volkszählung (Census Bureau) zur allgemeinen Nutzung freigegeben hat.

Kommerzielle Karten sind meist teuer und nur unter einer einschränkenden Lizenz erhältlich. Sie verbietet in der Regel die Weitergabe an andere oder die Veröffentlichung im Internet. Sogar die Geodaten, die Gemeinden und Landesvermessungsämter mit öffentlichen Geldern gesammelt haben, stehen der Allgemeinheit nicht zur Verfügung. Anders in den USA: Von Bundesbehörden gesammelte Daten stehen automatisch in der „Public Domain“. Das gilt unter anderem für die erwähnten TIGER-Daten und die Satellitenbilder der NASA.

Google Maps, Yahoo Maps und andere Anbieter erlauben zwar das Einbinden ihrer Karten in eigene Webseiten, schränken aber die Nutzung erheblich ein. So ist der Zugriff auf die Karten nur über die API erlaubt; man darf zum Beispiel keinen Ausdruck weitergeben. Google verbietet zudem die Nutzung auf passwortgeschützten Seiten und behält sich vor, jederzeit Werbung auf den Karten zu schalten.

Lizenz für beliebige Nutzung

Das OpenStreetMap-Projekt benutzt dagegen die Lizenz Creative Commons Attribution-Share Alike [c]. Sie erlaubt eine beliebige Nutzung, wenn man den Urheber nennt und anderen die gleichen Rechte an einem daraus abgeleiteten Werk einräumt. Eine kommerzielle Nutzung ist möglich. Die CC-Lizenzen wurden allerdings für Schriftwerke oder Musikstücke und dergleichen entworfen; ihre Interpretation in Bezug auf Geodaten ist noch unklar.

Eine MySQL-Datenbank speichert die mehrere GByte großen Kartendaten des OSM-Projekts. Einmal wöchentlich erstellen die Betreuer daraus einen Abzug mit dem aktuellen Datenbestand der ganzen Welt, das sogenannte Planet File, und stellen es zum Herunterladen zur Verfügung. Zusätzlich gibt es täglich und neuerdings stündlich Dateien mit den letzten Änderungen.

Die Daten liegen in einem OSM-spezifischen XML-Format vor. Die üblicherweise für geografische Informationssysteme (GIS) verwendeten Formate sind nicht geeignet, da sie auf einem anderen Datenmodell basieren. Der Export von OSM-Daten in GIS-Formate ist natürlich möglich, dabei gehen aber Teile der Information verloren.

Abweichend von typischen GIS-Datenmodellen kennt OpenStreetMap nur drei Datentypen: *Nodes, Ways* und *Relations*. Zur Identifizierung der Objekte dient eine eindeutige, unveränderliche ID. *Nodes* beschreiben genau einen Punkt auf der Erde mit seinen Koordinaten, beispielsweise einen Briefkasten. *Ways* modellieren Linien und Flächen; ein Way besteht aus einer geordneten Liste von mindestens zwei Nodes, die den Linienverlauf beziehungsweise den Umriss einer Fläche festlegen. Erst aus den einem Way zugeordneten Tags ergibt sich, ob es sich um ein Linien- oder ein Flächenobjekt handelt. Ways beschreiben zum Beispiel Straßen und Wege, Eisenbahntrassen, Flüsse, Seen und Wälder.

Relations definieren komplexe Beziehungen zwischen Objekten. Sie fanden erst im Oktober 2007 Einzug in das OSM-Datenmodell, und ihre Nutzung ist derzeit noch in der Entwicklung begriffen. Eine Anwendung sind Abbiegerelationen, wie sie für das Routing notwendig sind. Damit lässt sich beispielsweise angeben, dass man von Straße A kommend an Kreuzung K in die Straße B nicht links abbiegen darf.

iX-TRACT

- OpenStreetMap ist ein Wikipedia-artiges Projekt mit dem Ziel, Geodaten für eine Weltkarte zu sammeln und kostenlos unter einer freien Lizenz herauszugeben.
- Es gibt große Fortschritte, aber Vollständigkeit und Qualität der Karten unterscheiden sich regional noch stark.
- Verschiedene Programme ermöglichen es jedem, die Daten zu editieren oder passende Karten für eigene Anwendungen zu erzeugen.

Bei OpenStreetMap mitmachen

OpenStreetMap lebt davon, dass jeder Daten aus den Gegenden beiträgt, die er kennt. Das ist zwar einfach, aber ein paar kleine Hürden sind zu überwinden. Dazu gehört als Erstes der für das Ändern von OSM-Daten nötige Account. Ihn gibt es auf www.OpenStreetMap.org bei „sign up“. Nach der Anmeldung stellt man auf der Karte den relevanten Ausschnitt ein und klickt auf den „Edit“-Reiter. Er startet den Flash-Editor *Potlatch* zum Ändern und Ergänzen der Geodaten, der alle Änderungen sofort in die Datenbank schreibt.

*Potlatch*s Bedienung ist gewöhnungsbedürftig und begeistert nicht jeden. Eine Alternative bildet der deutlich mächtigere Editor JOSM [i]. Er ist in Java geschrieben und funktioniert daher unter allen Betriebssystemen. Nach seinem Start lädt man per „File -> Download“ einen Ausschnitt der Daten vom Server herunter. Die Bedienung ähnelt der eines Vektor-Zeichenprogramms. Über das Presets-Menü oder den Properties-Dialog ändert man die Tags der Datenobjekte. Welche üblich sind, beschreibt die Seite „De:Map Features“ im OSM-Wiki. Änderungen wirken sich erst nach dem Hochladen per „File -> Upload to OSM“ auf die OSM-Daten aus.

So lassen sich Geodaten zwar ändern, zum Beispiel ein fehlender Straßenname ergänzen. Daten für ein bisher leeres Gebiet müssen jedoch irgendwoher kommen. Eine Quelle kann ein GPS-Gerät sein, das den gefahrenen Weg in einem sogenannten Track aufzeichnet. Direkt im GPX-Format oder von *GPSBabel* [j] dorthin konvertiert, dient er als Hintergrund für JOSM (via „File -> Open“). Darauf zeichnet man manuell die Straßen und Wege nach und versieht sie mit Tags. Wer sich unterwegs Notizen gemacht hat (zum Beispiel auf einem Stück Papier oder mit der Aufnahmefunktion eines MP3-Players), kann zusätzlich Straßennamen, die Richtung von Einbahnstraßen, die Position von Kirchen und Briefkästen et cetera eintragen.

Eine Alternative dazu ist das Abzeichnen von Satellitenbildern. Mögliche Vorlagen sind die Landsat-Bilder der NASA, die allerdings nur eine geringe Auflösung haben, oder die Satelliten- oder Luftbilder von Yahoo. Yahoo hat erklärt, dass das Abzeichnen seiner Luftbilder (nicht jedoch der Karten) für OSM-Zwecke zulässig sei.

Potlatch-Benutzer bekommen die Yahoo-Bilder automatisch im Hintergrund angezeigt. JOSM-Anwender müssen erst das WMS-Plug-in für Landsat-Bilder beziehungsweise das YWMS-Plug-in für Yahoo-Bilder installieren. Dann steht ein WMS-Menü zur Verfügung, mit dem sie die Bilder für den aktuell angezeigten Ausschnitt anfordern können.

Auch der Modellierung von Flächen mit Löchern dienen Relations, die hier auf die Ways für die inneren und äußeren Ringe verweisen.

Tags definieren Eigenschaften

Beliebige Tags der Form *Schlüssel=Wert* können Nodes, Ways und Relations Eigenschaften zuordnen. Zum Beispiel könnte eine Bundesstraße die Tags *highway=primary, ref=B3* und *name=Durlacher Straße* besitzen. *leisure=park* markiert einen Park, *amenity=post_box* einen Briefkasten. Eisenbahn-, S-Bahn- und Straßenbahntrassen bekommen alle Tags, die den Schlüssel *railway* verwenden. Es gibt eine Fülle an Zusatztags, die weitere Attribute beschreiben, etwa die zulässige Höchstgeschwindigkeit bei Straßen oder *layer=1* für Brücken zur eindeutigen Festlegung, welche Straße über welcher verläuft.

Das Datenmodell ist also recht primitiv, damit aber leicht verständlich und flexibel. Der Großteil der Information steckt in den Tags, deren Menge ständig wächst. Das Projekt hat darauf verzichtet, von vornherein eine definitive Liste aller Tags vorzugeben, stattdessen „erfinden“ die Teilnehmer neue, wenn jemand sie brauchen kann.

Ein wesentlicher Vorteil von OSM gegenüber anderen Kartendiensten im Internet ist der Zugriff auf die Rohdaten. Anwender können daher selbst entscheiden, welche Objekte auf einer Karte in welcher Form erscheinen sollen. Was sie dazu brauchen, ist ein sogenannter Renderer, der aus den Rohdaten eine ansprechende Karte erzeugt. Davon gibt es mehrere, am häufigsten kommen die Programme *Osmarender* [d] und *Mapnik* [e] zum Einsatz.

Osmarender ist ein XSLT-Skript, das SVG (Scalable Vector Graphics) aus dem OSM-XML-Format erzeugt. *Mapnik* erstellt Bitmap-Karten, braucht dazu allerdings eine PostgreSQL-Datenbank, in die man die OSM-Daten importieren muss. Es ist deutlich schneller als *Osmarender* und kommt mit größeren Datenmengen zurecht.

Beide Renderer legen in einer Regeldatei die Darstellung der Objekte fest. Im Web gibt es zum Beispiel für Radfahrer die Cycle Map [f]. Sie stellt Fahrradrouten wesentlich prominenter dar als Autobahnen.

Neben eigenen Karten sind viele andere Anwendungen der OSM-Daten denkbar. Für die Nutzung in klassischen Geoinformationssystemen gibt es den Konverter *Osmexport*, [g] in das Shape-Format. Unter anderem lassen sich die Daten zur Straßennavigation verwenden, zum Beispiel mit dem Linux-Programm Navit [h]. Noch können Qualität und Vollständigkeit der Daten sowie die zur Verfügung stehende Navigationssoftware mit der kommerziellen Konkurrenz allerdings nicht mithalten.

In vielen Bereichen sind die OSM-Daten heute noch unvollständig, trotzdem stellen sie eine der größten und interessantesten Sammlungen freier Geodaten dar. Für viele Anwendungen können sie in Zukunft eine ernstzunehmende Alternative zu proprietären Kartendaten sein. (ck)

JOCHEN TOPF

arbeitet als freiberuflicher Entwickler und Berater. Er ist Koautor des im Februar 2008 erschienenen Buches „OpenStreetMap: Die freie Weltkarte nutzen und mitgestalten“.



Onlinequellen

[a] OpenStreetMap-Projekt	www.OpenStreetMap.org
[b] Vergleich zwischen OSM- und Google-Karten	geo.topf.org/comparison/index.html
[c] Creative Commons	www.creativecommons.org
[d] Osmarender	wiki.OpenStreetMap.org/index.php/Osmarender
[e] Mapnik	www.mapnik.org
[f] OSM Cycle Map	www.gravitystorm.co.uk/osm/
[g] Osmexport	osmlib.rubyforge.org/osmlib-export/
[h] Navit	www.navit-project.org
[i] JOSM	josm.OpenStreetMap.de
[j] GPSBabel	www.gpsbabel.org



Collaboration-Lösungen für KMU

Neu gruppiert

Christian Böttger, André von Raison

Auch in kleineren Unternehmen nimmt der Druck zu, die Zusammenarbeit zwischen den Mitarbeitern unterschiedlicher Bereiche zu verstärken. Mit dem Einsatz von Groupware hoffen viele, Synergien zu nutzen und mehrfache Datenhaltung zu vermeiden.

Schon vor gut einem Jahr hatte sich *iX* mit einer Studie [1] des Themas Groupware angenommen. Parallel dazu befassten sich zwei Artikel in der Ausgabe 4/2007 mit dem gleichen Komplex, damals aber mit dem Fokus auf den Einsatz in großen Unternehmen [2, 3]. Inzwischen wächst aber auch in kleineren Firmen der Druck, ihre verschiedenen Unternehmensbereiche besser respektive überhaupt miteinander zu vernetzen und beispielsweise die Datenhaltung und das Termin-Management zu zentralisieren.

iX nahm das als Anlass, Groupware-Anbieter mit dem Fokus Einsatz in kleinen und mittleren Unternehmen (KMU) zu befragen. Fünfzehn Hersteller schickten die ausgefüllten Fragebögen zurück, die Zusammenfassung der Ergebnisse finden sich in der Tabelle am Ende des Artikels, die ausschließlich auf den Herstellerangaben beruht. Fast alle Anbieter der letztjährigen Artikel fühlen sich auch für den Sektor KMU zuständig. Nur von IBM respektive Lotus kam keine Antwort, vielleicht aufgrund der vorösterlichen Urlaubszeit. Für die Tabelle griffen wir daher auf die gegebenenfalls nicht mehr ganz aktuellen Daten der Groupware-Studie [1] zurück.

Einige – vor allem Open-Source-basierte – Produkte gibt es nicht nur als eigenständige Software, sondern auch als integrierte Bestandteile von Komplettpaketen. *iX* wird in der nächsten Ausgabe einige dieser Rundum-glücklich-Lösungen mit dem Platzhirsch in diesem Segment, Microsofts Small Business Server, vergleichen. Die Redmonder beanspruchen für ihre Groupware-Komponente Exchange immerhin einen Marktanteil von 59 % in Deutschland. Das schlägt sich indirekt auf die Exchange-Alternativen nieder: Nur ein gutes Drittel der Pakete läuft auch unter Windows.

Besonderheiten der Zielgruppe KMU

Kleinere Firmen haben in Sachen IT besondere Anforderungen. Hier fehlt es zum einen oft an dediziertem Know-how und zum anderen an der Zeit zur Betreuung komplexer Systeme wie einer Groupware. Ein wichtiges Kriterium war daher die Verfügbarkeit eines professionellen Ansprüchen genügenden Service- und Support-Angebots. Dadurch bleibt eine Reihe reiner Open-Source-Projekte wie phpGroupware, PHProject oder die Horde-Groupware hier außen vor. Beim freien Kolab sieht die Sache anders aus: Hier haben sich einige Dienstleister aus dem Open-Source-Umfeld zusammengetan und kümmern sich als Kolab-Konsortium sowohl um die Serviceangebote als auch um die Koordination der Weiterentwicklung. Auch spielt die Frage der Lokalisierung für das hier betrachtete Einsatzszenario eine nicht unerhebliche Rolle.

Welches Produkt für wen infrage kommt, hängt natürlich nicht nur vom Serviceangebot, sondern in erster Linie von den Präferenzen eines Unternehmens ab. Das Betriebssytemspektrum reicht von den PC-verwurzelten wie Windows und Linux bis hin zu den bei KMU vermutlich eher weniger stark verbreiteten Plattformen S/390 und AS/400. So laufen von den 15 Kandidaten bis auf Exchange alle auch unter Linux. Lediglich sechs lassen sich unter Windows betreiben – genauso viele wie unter Mac OS X. Selbst Unix-Anhänger können sich zwischen mehr Alternativen (sieben) entscheiden. Clientseitig verlagert sich die Verteilung wieder in

Richtung Redmond: Keines der Produkte verschließt sich der Realität der überwiegend mit Windows ausgestatteten Arbeitsplatz-PCs in den Unternehmen und umgeht, wie weiter unten beschrieben, viele Hakeleien mit der Anbindung mobiler Endgeräte.

Leider ist der Begriff „Groupware“ nirgends eindeutig definiert – jeder Hersteller versteht etwas anderes darunter. Um eine gewisse Vergleichbarkeit der Herstellerangaben zu gewährleisten, benutzt dieser Artikel eine eigene Begriffsbestimmung. Eine Groupware ist ein E-Mail- und Kommunikationssystem, das folgende grundlegende Inhalte bereitstellt: Adressen und Kontakte, Aufgaben, E-Mail, gemeinsame Folder, Kalender sowie Notizen. Diese Anforderung erfüllen alle Produkte in der Tabelle.

Eine Gelegenheit zur Differenzierung ergibt sich für die Hersteller bei darüber hinausgehenden Funktionen, bei denen teils gravierende Unterschiede auftreten. Einige legen großen Wert auf Abgleich mit möglichst vielen mobilen Geräten, andere setzen den Schwerpunkt beispielsweise auf breite Unterstützung für Unified-Messaging- oder Portalfunktionen. Auch in Sachen Standardschnittstellen treten deutliche Unterschiede zutage. So fehlt erstaunlich vielen Produkten die Option, die verschlüsselten Varianten von Standardprotokollen wie IMAP4S oder POP3S einzusetzen.

Ausgeprägte strukturelle Ähnlichkeiten

Manche Groupware-Systeme liefern keine Clients mit, sie setzen hierfür ausschließlich auf Outlook. Andere wiederum haben eigene Fat Clients für unterschiedliche Plattformen im Angebot, während ein weiterer Teil der Anbieter sich dem reinen Webzugriff verschworen hat.

Abbildung 1 zeigt den grundsätzlichen Aufbau vieler Groupware-Systeme und deren Zusammenspiel mit den Clients. Die technische Ausführung variiert natürlich stark, die Variationen reichen von der klassischen monolithischen Server-Applikation bis hin zum J2EE-Applikationsserver mit AJAX-basiertem Web-2.0-Zugriff. Grundsätzlich jedoch befindet sich die eigentliche Groupware-Software auf einem (oder mehreren) Servern. Die verarbeiteten Daten werden dort gespeichert, oft in SQL-Datenbanken, manchmal jedoch auch im Dateisystem in eigenen Datenstrukturen. Für den E-Mail-Austausch nach draußen ist ein SMTP-Server nötig. Dieser Mail Transport Agent (MTA) ist manchmal ins System integriert, manchmal greifen die Anbieter auf Fremdprodukte zurück. Oft bieten die Mailserver-Komponenten auch POP3 und IMAP an, sodass reine Mailclients zumindest auf die E-Mails zugreifen können. Viele Systeme realisieren ihren Verzeichnisdienst über LDAP. Daneben existiert einen ganzer Zoo anderer Schnittstellen, um auf die weiteren Daten außer E-Mail und Adressen, beispielsweise Termine, zugreifen zu können: CalDAV, WebDAV, GroupDAV, SOAP, XML-RPC. Für darüber hinausgehende Aktivitäten kommen in der Regel proprietäre Protokolle zum Einsatz.

Potenzielle clientseitige Stolperfallen

Die Clients sind über ein Netz angebunden. Am einfachsten haben es die reinen Weblösungen: Sie kommunizieren meist ausschließlich über HTTP oder HTTPS. Bei den Fat Clients kommen meist mehrere Protokolle zum Einsatz, was beispielsweise den Zugriff von Remote Clients auf das System erschwert. Ein solcher Protokollzoo kann schnell zum sicherheitstechnischen Albtraum geraten. Eine Besonderheit stellt Outlook dar. Microsofts Client funktioniert am besten, wenn es mit dem Server über das (proprietäre) MAPI (Mail-API) kommunizieren kann. Alle vorgestellten Groupware-Systeme realisieren dies, indem sie lokal auf den Clients ein Outlook-Plug-in installieren, das Outlook gegenüber die MAPI anbietet und zusätzliche Menüpunkte in Outlook einfügt, wie die Konfiguration der Netzparameter des Servers, Abwesenheitsschaltungen, serverbasierte Regeln und Filter et cetera. Zur Groupware hin kommunizieren diese Plug-ins dann entweder über Standardprotokolle, tunneln über HTTP oder verwenden proprietäre Protokolle. Daneben kann Outlook aber auch von Haus aus zumindest für E-Mail und Adressen direkt über Standardprotokolle mit externen Servern Daten austauschen, also über SMTP, POP, IMAP (neuere Versionen), LDAP & Co.

Sobald mobile Endgeräte ins Spiel kommen, wird die Situation noch komplizierter. In der Regel kommunizieren die Geräte über proprietäre Protokolle (über serielles Kabel, Bluetooth, IrDA (Infrarot) oder TCP/IP) mit einer Synchronisierungssoftware auf dem Client-Rechner. Die Software verbindet sich dann entweder als Plug-in oder via MAPI mit Outlook. Von dort wandern die Daten in das Groupware-System. Es besteht aber auch die Möglichkeit, über das SyncML-Protokoll direkt das mobile Endgerät mit dem Groupware-System abzugleichen, ohne einen Client wie Outlook dazwischenzuschalten. Dies setzt allerdings eine direkte TCP/IP-Verbindung zwischen Endgerät und Server voraus.

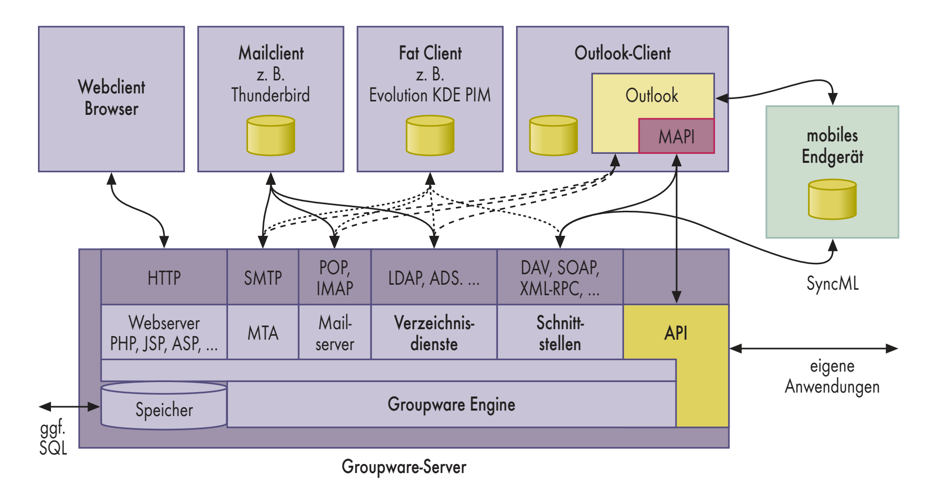
Systeme ohne Fat Client, also reine Weblösungen, bieten grundsätzlich keine lokale Datenhaltung. Dies ist kein Problem, solange man eine ständige, hinreichend breitbandige HTTP(S)-Verbindung zum Server sicherstellen kann, sei es im LAN oder über das Internet – im letzteren Fall aber bitte verschlüsselt. Die Browser-Lösungen haben prinzipiell Schwierigkeiten, mobile Endgeräte wie PDAs und MDAs zu synchronisieren.

Outlook als generischer Windows-Client

Letzteres machen sich die Fat-Client-Lösungen meist recht einfach: Sie unterstützen oft nur Outlook als Client und überlassen es den proprietären

iX-TRACT

- Vor allem im Bereich KMU ist der Begriff Groupware in der Praxis nicht mehr zwingend ein Synonym für Microsofts Exchange.
- Das Spektrum der Angebote reicht von klassischen Client/Server-Architekturen mit Fat Clients über reine Weblösungen bis hin zu J2EE-Applikationsservern mit AJAX-Clients.
- Open-Source-Pakete greifen meist auf Konnektoren von Drittanbietern für die Anbindung von Outlook als Client zurück.



Ein Groupware-Server bietet den Clients oft unterschiedliche Verbindungsmöglichkeiten – ein Grund für die Komplexität des Gesamtsystems (Abb. 1).

Tools des MDA/PDA-Herstellers, ihre Geräte mit Outlook zu synchronisieren. Fat Clients haben den Vorteil, dass sie eine lokale Datenhaltung betreiben (können) und somit auch offline zur Verfügung stehen.

Fast alle Systeme, die Fat Clients unterstützen, unterstützen auch Outlook. In jedem Fall ist die lokale Installation eines sogenannten Konnektors nötig. Manche Teile von Outlook jedoch, die beim Betrieb an einem Exchange-Server als integrale Bestandteile erscheinen, sind gar keine generischen Outlook-Eigenschaften. Dazu zählen unter anderem die beliebten Assistenten, allen voran der Abwesenheitsassistent und der Zugriff auf öffentliche Ordner. Diese Teile muss der Konnektor zur Verfügung stellen. Die Ausprägung dieser Konnektor-Komponenten variiert von Lösung zu Lösung stark und reicht von „nahezu vollständig“ bis hin zu „nicht vorhanden“.

Für eine fundierte Entscheidung über die Eignung einer Groupware müssen Interessenten zunächst die eigenen Anforderungen festlegen. An erster Stelle steht die Frage nach dem Funktionsumfang, die auch eventuelle erweiterte Fähigkeiten wie CRM, Projektmanagement, CTI-Anbindung, Instant Massaging, Intranetportal oder eine Workflow-Komponente berücksichtigen sollte.

Ebenso wichtig ist die Zahl der zu versorgenden Arbeitsplätze, wobei man hierbei durchaus auch einen Gedanken an die nähere Zukunft verwenden sollte. Neben der Zahl spielt auch deren Ausstattung gegebenenfalls eine Rolle, eine Client/Server-Architektur mit Fat Clients hat andere Anforderungen als ein Web-Ansatz. Wie oben ausgeführt, beeinflussen eventuell zu verwendende mobile Endgeräte diese Entscheidung. Ist ein externer Zugriff per Internet vorgesehen, sollte man sich für Fat Clients gleich nach einer VPN-Lösung umsehen.

Kontaktfreudigkeit als Entscheidungskriterium

Soll sich die Groupware an vorhandene Anwendungssysteme (ERP, CRM, …) koppeln oder muss sie mit Verzeichnisdiensten (LDAP, ADS, …) zusammenarbeiten, liefert ein Blick in die Zeile der vorhandenen Schnittstellen wichtige Informationen.

Besonders sorgfältig muss man bei der Migration von einem schon vorhandenen Groupware-System vorgehen. Viele der genannten Produkte bieten keine oder nur rudimentäre Möglichkeiten, Daten aus anderen Systemen zu übernehmen. Insbesondere die Rollen und Rechte der vorhandenen Nutzerkonten lassen sich selten in ein neues System übernehmen.

Und nicht zu vergessen die Frage, in welche IT-Landschaft sich die Groupware einbetten soll. Der tatsächliche Nutzen einer Groupware hängt stark von der Akzeptanz durch die Mitarbeiter ab. Ein eingeführtes Outlook abzulösen, erfordert vermehrt Schulungen und Überzeugungsarbeit.

Unter Umständen erfolgt eine Entscheidung nicht nur aufgrund technischer Kriterien. Auch die Lizenzkosten sind nicht unbedingt der maßgebende Faktor. Bei der Wahl zwischen freier oder proprietärer Software kann es in gewisser Weise eine geschäftspolitische Entscheidung sein, denn mit freier Software sind andere Arbeitsabläufe und Prozesse verbunden.

Zwar bietet freie Software viele Vorteile, beispielsweise fallen die Lizenzkosten weg. Damit sinkt die Eintrittsschwelle. In allen Fällen, in denen eigene Erweiterungen nötig sind, lassen sich diese problemlos durchführen. Aber da es nicht einen einzelnen Hersteller gibt, muss man im IT-Management andere Prozesse einführen: Die IT-Abteilung muss sich stärker mit der Software beschäftigen. Geld muss man bei jeder Software einsetzen – aber in unterschiedlicher Weise: nicht für Lizenzen wie bei proprietärer Software, sondern verstärkt für Arbeitszeit und Ausbildung der Mitarbeiter wie bei den freien Pendants.

Fazit

Für KMU existiert ein gut sortiertes Angebot von Groupware-Paketen, die sich im Einzelnen bei den über die Grundausstattung hinaus angebotenen Funktionen teils deutlich voneinander unterscheiden. Da eine Entscheidung für eine Groupware unter Umständen tief in betriebliche Abläufe hineinwirkt, sollten sich potenzielle Kunden, beispielsweise anhand der im Artikel vorgestellten Kriterien, ihre Anforderungen verdeutlichen. Mit diesen Informationen und anhand der Daten in der Tabelle kann man schnell fündig werden – und die Lösung muss keinesfalls immer Exchange heißen.

CHRISTIAN BÖTTGER

arbeitet als freiberuflicher IT-Berater und Projektmanager mit Schwerpunkt in den Bereichen Groupware, Projektmanagement und freie Software.

Literatur

[1] C. Böttger (Hrsg.), K. Detken, A. Erbe, L. Grunwald, K. Mönickes, C. Schommer, M. Wagner; iX-Studie; Groupware; Kommerzielle und Open-Source-Groupware-Systeme im Vergleich; Heise Zeitschriften Verlag, 2007

[2] Christian Böttger, Jan Geisbauer; Groupware I; Viergestirn; Collaboration-Lösungen für große Umgebungen; *iX* 4/2007, S. 50

[3] Christian Böttger; Groupware II; Gruppenweise; Enterprise-taugliche Groupware-Lösungen für Linux; *iX* 4/2007, S. 58

Groupware für KMU

Produkt	Communigate Pro 5.2	David.zehn! Business Edition	Exchange 2007	Groupwise 7.0.3
Anbieter	Communigate Systems, Division of Stalker Software GmbH	Tobit.Software AG	Microsoft Deutschland GmbH	Novell
E-Mail	europe@communigate.com	hallo@tobit.com	k. A.	kontakt-de@novell.com
WWW	www.communigate.com	www.tobit.com	www.microsoft.com	www.novell.de
installierte Basis	12 000 Kunden, 130 Mio Mail Accounts	> 4 Mio	im hohen Millionenbereich	35 Mio
Dienstleistungen [1]	c, d, e, f	a – g	d, e, f, g	a – g
Basisdaten				
Sprache[2] Server/Administration/Doku	DE, EN, FR, weitere/EN/EN	DE, EN, FR, weitere/DE, EN/ DE, EN	DE, EN, FR, weitere/DE, EN, FR, weitere/DE, EN, FR, weitere	DE, EN, FR, weitere/DE, EN, FR, weitere/DE, EN, FR, weitere
Architektur	Client/Server mit Webanbindung, eigenes Flash-UI	Client/Server mit Webanbindung	Client/Server mit Fat Client und Webzugriff	Client/Server mit Fat Client und Webzugriff
Outlook-Support/MAPI/OWA/Sync only/ Nachrichten via Adressbuch/MAPI extern	ab 98/✓/–/✓/✓/–	– /(✓ Simple MAPI)/–/–/–/ (✓ Simple MAPI)	ab 2002/✓/✓/✓/✓/✓	ab 98/✓/–/–/–/✓
eigene/andere FAT Clients	Flash-basiertes UI/Evolution, jeder standardbasierte	Windows [Mobile], Java/–	Windows, Mac/–	Windows, Linux, Mac/Evolution, Kontact, andere via POP, IMAP oder SOAP
eigener Web-Client/Umfang	✓/E-Mail, Kalender, Adressen, Shared Folders, (IM, VoIP, Presence nur Flash UI)	✓, vollständig	✓/siehe Hersteller-WWW	✓/E-Mail, Kalender, Adressbuch, Dokumente, Termine
Betriebssysteme Server	Windows, Linux (auch PowerPC, IA64), Unix, S/390, AS/400, Mac OS X, andere	Win bis 2003, Linux 2.4.x bis 2.6.18	ab Windows NT	Windows ab 2003, ab SLES 9, Netware ab 5.x
Betriebssysteme Client	Windows, Linux/Unix, Mac OS X	Windows ab 2000	Windows ab 2000, Mac	Windows ab 2000, Linux, Mac
Anforderungen Server	ab Pentium, 512 MByte RAM	Voraussetzung des OS	1 CPU-Core, 2 GByte RAM und 100 GByte HD	x86 oder x86_64 mit 32-Bit-Mode
dito Client	keine Vorgaben	Voraussetzung des OS	1 CPU-Core, 256 MByte RAM, 50 GByte HD	keine Vorgaben
dito Netz	keine Vorgaben	100 MBit	5 KBit/s	k. A.
Protokolle und Formate				
Protokolle	POP3[S], IMAP4[S], SMTP[Auth], TLS/ SSL, LDAP[S], MAPI vollständig, andere	POP3[S], IMAP4[S], SMTP[Auth], TLS/SSL, Simple MAPI, andere	POP3, IMAP4, SMTP[Auth], TLS/ SSL, LDAP, MAPI vollständig	POP3[S], IMAP4[S], SMTP[Auth], TLS/ SSL, LDAP[S], MAPI vollständig, andere
Importformate	CSV, TXT, LDIF, vCard, iCal, PST (ab 98)	CSV, TXT, vCard, iCal, PST (ab 2000), VCF, Word-Makro	TXT, vCard, iCal, PST	CSV, vCard, iCal, PST
Exportformate	CSV, TXT, LDIF, vCard, iCal, PST (ab 98)	CSV, TXT, vCard, iCal, eml, VCF SKL, XLS	vCard, iCal, PST	csv, vCard, iCal
Verzeichnisdienst Authentifizierung/ mitgeliefert	LDAP/LDAP	–/–	AD/–	LDAP, eDirectory/LDAP, eDirectory
Single-Sign-On	LDAP	AD, NT-DOM, LDAP, NIS[+], eDir	AD	LDAP, eDirectory
SQL-Schnittstelle	–	✓	✓	–
eigener MTA/andere nutzbar	✓/–	✓/✓ (alle SMTP basierten)	✓/–	✓/–
Unified Communication	Fax[3], Voicemail, VoIP, Videokonferenz, IM, Shared Folder, Shared Calendar	Fax, Voicemail, VoIP, SMS	Fax, Voicemail, VoIP	Fax, Voicemail, VoIP
Außenanbindung				
Anbindung an CRM/ERP/EAI o. SOA	–/–/–	✓/✓/–	✓/✓/–	–/✓ (SAP Netweaver)/–
maximale Konten/parallele Benutzer pro Server	k. A.	5000/5000	< 150 000/< 150 000	10 000/5000
Quotas/Clusterfähigkeit	✓/✓	k. A./–	✓/✓	✓/✓
offline-fähig/Synchronisation via	–/Outlook, Activesync, Airsync, SyncML	✓/Activesync, eigenständig	✓/Outlook, Activesync, Entourage	✓/Activesync, eigenständig
mobile Endgeräte	PalmOS, Windows Mobile, Symbian, Blackberry	Windows Mobile, Symbian, Blackberry, iPhone	Windows Mobile	(SyncML)PalmOS, Windows Mobile, Symbian, Blackberry
zentrales Backup/inkl. Einzelereignisse	✓/✓	✓/✓	✓/(✓)[3]	✓/✓
Patches automatisch/manuell/individuell	–/✓/–	✓/✓/–	✓/✓/✓	–/✓/✓
Spam-Schutz intern/extern	✓/ Mailshell, Cloudmark	✓/–	✓/EHS	✓/Gwava, Messaging Architects u. a.
Virenschutz intern/extern	✓/McAfee, Kaspersky, Sophos, Clamav	✓/–	✓/EHS	✓/Gwava, Messaging Architects u. a.
Migrationshilfen	✓, eigene Tools	✓, eigene Tools	✓, eigene und fremde Tools	✓, eigene Tools
Datenübernahme lokal/zentral/ Exchange | Outlook/Notes | Domino/ Groupwise/andere	✓/✓/✓/–/–/via IMAP oder POP	–/–/✓/–/–/–	✓/✓/✓/✓/–/–	✓/✓/✓/–/✓/–
übernehmbare Daten[5]	a, c, d, e, f, g, h, i	d, f, g, h	a, b, d, e, f, g, h	a, d, f, g, h
Funktionsumfang[6, 7]	GF[6], f, g, h, k, l, n, o, p	GF[6], a, b, d, f, g	GF[6], d, f, h, i, j, k	GF[6], a – p
Preise				
Lizenz/Abrechnung	proprietär/pro Server oder User	proprietär/pro Server, User, Transaktion	proprietär/pro Server, User, Device	proprietär/flat, pro Organisation, User
Kosten Server/User/Webclient	899 € (25 User)/gestaffelt/0 €	495 € (5 User)/ab 40 €/ ab 60 €	abhängig vom Lizenzmodell	–/134 €/31 €
Wartung jährlich/1. Jahr inklusive	161 €/–	k. A./–	abhängig vom Lizenzmodell	34 € pro User/–

[1] Dienstleistungen: a Produkt- b Anwender- c Administratorenschulung, d Einführungs-, e Prozess-, f Integrationsberatung, g weitere [2] ISO-Länderkennung [3] nur über Drittanbieter
[4] über Konnektor [5] Datenarten: a Nutzerkonten, b Benutzereinstellungen, c Nutzergruppen, d E-Mails, e E-Mail-Verteiler, f Adressen, g Termine, h Aufgaben, i gemeinsame Ordner, j Notizen
[6] GF – Grundfunktionen: Adressen/Kontakte, Aufgaben, E-Mail, gemeinsame Folder, Kalender, Notizen [7] erweiterte Funktionen: a Projektmanagement, b Dokumentenverwaltung, c Helpdesk, d Workflow, e CRM, f Volltextsuche, g CTI-Anbindung, h Portalfunktion, i Shared Workplace, j Foren, k Usenet, l Instant Messaging, m Wiki, n Wissensdatenbank, o Umfragesystem, p Intranetportal

InstantOGo Advanced Server Edition 2.2	Intranator Business Server 5.0.3/ Groupware Connector 1.2.1	Kerio Mail Server 6.5	Kolab Server 2.2RC2
Skyrix Software AG	Intra2net AG	Kerio Technologies Inc.	Intevation GmbH
sales@skyrix.de	info@intra2net.com	info@kerio.com	info@intevation.de, info@kolab-konsortium.de
www.skyrix.de	www.intra2net.com/de	www.kerio.de	www.intevation.de, www.kolab-konsortium.de
circa 500	2100 Installationen, 53 000 Benutzer	> 20 000	nicht ermittelbar, da freie Software
a – g	a, c, d, f	k.A.	a – f
DE, EN/DE, EN/DE, EN	DE, EN/DE, EN/DE	DE, EN, FR, weitere/DE, EN, FR, weitere/EN, weitere	DE, EN, FR, weitere/DE, EN, FR, weitere/DE, EN
Webanwendung mit Browser-Zugriff	Client/Server mit Fat Client und Webzugriff (AJAX)	Client/Server mit Webzugriff	Client/Server mit Fat Client und Webzugriff
ab 98/✓/–/–/–/–	ab 2000/✓/–/–/✓/✓	ab 98/✓/–/–/–/–	(ab 2000)[4]/(✓)[4]/–/–/(✓)[4]/–
–/Evolution, Kontact, Sunbird, Apple iCal	✓/Kontact	–/Evolution, Mailapp, Entourage, Sunbird	✓ (Kontact)/Evolution mit Einschränkungen, E-Mail-Clients
✓/E-Mail, Gruppenkalender, Ressourcenplanung, Dokumentenverwaltung, Kontakte, Aufgaben	✓/E-Mail, Kontakte	✓/vollständig	✓/Webmail, Kalender, Adressbuch, Aufgaben, Notizen, gemeinsame Ordner
eigenes Linux auf bootfähigem ISO-Image	Intranator Linux	Windows, Linux, Mac OS X ab 10.4	Linux, Unix mit OpenPKG-Support
beliebig, da Browser-basiert	Windows ab 2000, Linux	Windows ab 2000, Linux, Mac	Windows (via Konnektor), Linux, Unix, Mac OS X mit KDE-Support
Pentium ab 1,5 GHz, 1 GByte RAM, 30 GByte HD	1 GHz CPU, 512 MByte RAM, 40 GByte HDD	CPU 500 MHz, 256 MByte RAM/Mac: G4/G5, 256 MByte RAM oder Intel Core, 1 GByte RAM	circa 2 MByte pro gleichzeitig zugreifendem Nutzer, Festplatte circa 800 MByte zuzüglich Nutzerdaten
ab 500 MHz, 128 MByte RAM	Mindestanforderungen von Microsoft	keine Anforderungen	KDE-fähiger Client vermutlich ab 250 MByte RAM, für Windows: Outlook läuft
64 KBit/s (Client), 100 MBit/s	100 MBit/s	lediglich benötigt	Clients ab GSM (14 KBit/s) oder ISDN (64 KBit/s), Bandbreite für E-Mail
POP3[S], IMAP4[S], SMTP[Auth], TLS/SSL, LDAP[S]	POP3[S], IMAP4[S], SMTP[Auth], TLS/SSL, MAPI vollständig, andere	POP3[S], IMAP4[S], SMTP[Auth], TLS/SSL, LDAP[S], andere	POP3[S], IMAP4[S], SMTP[Auth], LDAP[S], TLS/SSL, LDAP[S], andere
CSV, TXT, LDIF, vCard, iCal	CSV, TXT, vCard, iCal, PST, Kolab XML	CSV, TXT, vCard, iCal, PST (ab XP), IMAP-to-IMAP, 4DMail, eigene Migrationstools	CSV, LDIF, vCard, iCal, PST (mit Konnektor), E-Mail als MBox oder Maildir
TXT, LDIF, vCard, iCal	CSV, TXT, vCard, iCal, PST, Kolab XML	TXT, iCal	CSV, TXT, LDIF, vCard, iCal, PST (mit Konnektor), E-Mail als MBox oder Maildir
LDAP/LDAP	–/k.A.	AD, NT-DOM, LDAP, eDirectory, Apple OpenDirectory, Own Database/–	AD, LDAP, eDirectory/LDAP (AD via 3rd Party)
k.A.	–	–	k.A.
✓	–	–	–
✓/Postfix	✓/–	✓/–	✓/nur zusätzlich
–	Fax	–	Fax, Voicemail, VoIP, Videokonferenz, IM, weitere möglich
–/–/–	–/–/–	✓(Metadex)/–/–, Own API	–/–/(–) Kolab ist quasi eine SOA
keine Begrenzung/500	konzipiert für 5 – 250 Benutzer	kein Limit der Software	>100 000/2000 – 3000
✓/✓	✓/–	✓/–	✓/✓
✓/Outlook, Sunbird	✓/Outlook (Hotsync, Activesync)	✓/Outlook, Activesync, DalDAV	✓/Outlook, Activesync, SyncML(Webclient), KPilot
PalmOS	PalmOS, Windows Mobile, Symbian	PalmOS, Windows Mobile, Symbian, Blackberry, iPhone	PalmOS, alle SyncML-fähigen
✓/✓	✓/✓	✓/✓	✓/✓
–/✓/–	✓/✓/–	–/✓/–	–/✓/–
✓/Kaspersky, Sophos	✓/–	✓/–	✓/✓
✓/Kaspersky, Sophos	✓/–	✓/Alwil, CA, Eset, Grisoft, Sophos, Symantec, ClamAV	✓/✓
✓, eigene Tools	✓, eigene Tools	✓, eigene Tools	✓, über Drittanbieter (imapsync, Toltec)
✓/✓/✓/–/–/–	✓/–/✓/–/–/–	✓/✓/✓/–/–/4DMail, Communigate Pro, IMAP-to-IMAP	✓/✓/✓/–/–/Open-Xchange
a, d, e, f, g, h	a, d, f, g, h, i	a, c, d, e, f, g	a, d, f, g, h
GF[6], a, b, e	GF[6], f (Volltextsuche)	GF[6], f (Volltextsuche)	GF[6], f, h teilweise, (j – o leicht ergänzbar)
GPLv2 (Zidelook proprietär)/flat, pro Server (Zidelook proUser)	gemischt/pro Server, User	proprietär/pro User	diverse Open-Source-Lizenzen, Konnektoren proprietär/entfällt
690 €/100 € (5 User)/–	490 € (10 User)/30 € / (Outlook-Anbindung) 0 €	374 € (10 User)/15 €/0 €	0 €/nur Konnektor-Lizenz/0 €
345 €/✓	Server (10 User) 350 €, Konnektor: 25% von Liste/✓	–/✓	jährliche Grundwartungskosten bei den Mitgliedern des Kolab-Konsortiums bei <10 000 Mailboxen 5 €/Mailbox sowie 5 €/Client

Groupware für KMU

Produkt	IBM Lotus Notes/Domin0 7.0.2	Open-Xchange Express Edition	PostPath Server 3.1.1	Scalix 11.3
Anbieter	IBM Deutschland GmbH	Open-Xchange Gmbh	PostPath Inc.	Scalix, Inc. – a Xandros Company
E-Mail	halloibm@de.ibm.com	info@open-xchange.com	info@postpath.com	info@scalix.com
WWW	www.lotus.de	www.open-xchange.com	www.postpath.com	www.scalix.com
installierte Basis	circa 125 Millionen	k.A.	k.A	1,5 Mio
Dienstleistungen[1]	a – f	k.A.	a – f	a, c, f
Basisdaten				
Sprache[2] Server/Administration/Dokumentation	DE, EN, FR, weitere/DE, EN, FR, weitere/DE, EN, FR, weitere	DE, EN, FR/DE, EN/DE, EN, FR	DE, EN, FR, JP/EN/EN	DE, EN, FR, weitere/DE, EN, FR, weitere/DE, EN, weitere
Architektur	Client/Server mit zusätzlichem Webzugriff (AJAX)	J2EE Application Server mit Webzugriff (AJAX)	J2EE Application Server mit Webzugriff (AJAX)	Webanwendung mit Fat Clients
Outlook-Support/MAPI/OWA/Sync only/Nachrichten via Adressbuch/MAPI extern	ab 98/✓/–/–/–/✓	ab 2003/✓/–/–/✓/–	ab 98/✓/–/–/–/✓	ab 98/✓/–/–/✓/✓
eigene/andere FAT Clients	✓/–	–/Evolution, Kontact, andere via vCard, iCal, WebDAV	–/Evolution, Thunderbird, Eudora	–/Evolution, Kontact, Thunderbird, Sunbird, Lightning, Apple Mail, iCal
eigener Web-Client/Umfang	✓/Standardkomponenten	✓/vollständig	✓/vollständig	✓/E-Mail, Kalender, Kontakte, Adressbuch, Regeln, Public Folder
Betriebssysteme Server	Windows, Linux, Unix, i5OS, zOS	Linux (Ubuntu 6.06, wird mitgeliefert)	Linux (RHEL/CENTOS 4.5, SLES 10)	Linux
Betriebssysteme Client	Windows, Linux, Mac OS X	Windows, Linux, Unix, Mac OS X	Windows, Linux	Windows, Linux, Unix, Mac OS X
Anforderungen Server	256 MByte – 512 MByte RAM, ab 1,5 GByte HD (je nach Plattform)	für 50 User: Athlon64x2/Core2 Duo, 2 GByte RAM	Pentium 4, 80 GByte HD, 2 GByte RAM	1 CPU, 2 GByte RAM, 10 GByte HD
dito Client	ab 128 MByte RAM	browserfähig (IE7, Firefox 2.x, Seamonkey ab 1.0)	keine Beschränkungen	1 CPU, 512 MByte RAM, 2 GByte HD
dito Netz	Client ab 64 KBit/s, 100 MBit/s	k.A.	100 MBit/s	Client: 64 KBit/s, weniger mit SmartCache, LAN, WAN
Protokolle und Formate				
Protokolle	POP3[S], IMAP4[S], SMTP[Auth], LDAP[S], TLS/SSL, MAPI, andere	POP3[S], IMAP4[S], SMTP[Auth], LDAP[S], TLS/SSL, andere	POP3, IMAP4, SMTP, TLS/SSL, MAPI vollständig	POP3[S], IMAP4[S], SMTP[Auth], TLS/SSL, LDAP[S], MAPI vollständig, andere
Importformate	TXT, LDIF, iCal, Lotus 1-2-3	CSV, vCard, iCal, PST	CSV, PST, MS Exchange Migration Tool	CSV, vCard, iCal, PST, Scalix Mailbox-Format
Exportformate	TXT, LDIF, Lotus 1-2-3	CSV, vCard, iCal, PST	CSV, PST, MS Exchange Migration Tool	CSV, vCard, iCal, PST, Scalix Mailbox-Format
Verzeichnisdienst Authentifizierung/mitgeliefert	LDAP/–	LDAP, eDirectory/–	AD/– (i. V.)	AD, NT-DOM, LDAP, NIS[+], eDirectory, Kerberos, Radius/LDAP
Single-Sign-On	AD, NT-DOM, Citrix, Tivoli	mit passendem Plug-in: jeder	AD	AD, Kerberos
SQL-Schnittstelle	✓	k.A.	–	✓
eigener MTA/andere nutzbar	✓/–	✓/✓	✓/–	✓ (nur für interne Mail)/Sendmail
Unified Communication	Fax, Voicemail, Videokonferenz	–	–	(✓)[3]
Außenanbindung				
Anbindung an CRM/ERP/EAI oder SOA	✓(Siebel)/✓(SAP-Konnektoren)/✓(via Webservices)	–	–	✓/(✓ via Outlook)/–
maximale Konten/parallele Nutzer pro Server	keine Beschränkungen/hardwareabhängig	bis zu 10 000/1000 – 2000	keine Beschränkungen/hardwareabhängig	bis 25 000/< 10 000
Quotas/Clusterfähigkeit	✓/✓	✓/✓	✓/✓	✓/✓
offline-fähig/Synchronisation via	✓/EasySync	✓/Outlook	✓/Outlook, Activesync	✓/Outlook, Activesync
mobile Endgeräte	PalmOS, Windows Mobile, Symbian, Blackberry, Nokia	– (geplant)	PalmOS, Windows Mobile, Symbian, Blackberry	PalmOS, Windows Mobile, Symbian, Blackberry, iPhone
zentrales Backup/inklusive Einzelereignisse	✓/✓	✓/✓	✓/✓	✓/✓
Patches automatisch/manuell/individuell	–/✓/–	✓/–/–	–/✓/–	–/✓/–
Spam-Schutz intern/extern	✓/✓	✓/✓	–/✓ alle gängigen	✓/Spamassassin
Virenschutz intern/extern	✓/✓	✓/✓	–/✓ alle gängigen	–/✓
Migrationshilfen	✓, eigene und 3rd-Party-Tools	✓, eigene Tools	✓, MS Exchange Migration Tool	✓, eigene Tools, EShuttle
Datenübernahme lokal/zentral/Exchange | Outlook/Notes | Domino/Groupwise/andere	✓/✓/✓/–/–/–	✓/✓/✓/–/–/Linux-Mail-Systeme	–/✓/✓/–/–/–	✓/✓/✓/✓/✓/Open-Xchange, IMAP, Sun
übernehmbare Daten[5]	a, b, d, e, f, g, h	a, d, f, g, h, i	a, b, c, d, e, f, g, h, i	a, c, d, e, f, g, h
Funktionsumfang[6, 7]	GF[6], a[3], b, c[3], d[3], e[3], f, g, i, j, k, i, p	GF[6], b, f, g, h	GF[6], a – p	GF[6], f (Volltextsuche)
Preise				
Lizenz/Abrechnung	proprietär/pro Organisation, User	GPL und proprietär/pro User	proprietär/pro User	proprietär, Scalix Public License basierend auf MPL/pro User
Kosten Server/User/Webclient	1295 € (25 User)/102 €/71 €	299 € (5 User)/35 €/0 €	ab 60 User frei/63 US-$/31 US-$	0 €/20 – 60 €/0 €
Wartung jährlich/1. Jahr inklusive	inklusive/✓	25% von Listenpreis/✓	22% vom Listenpreis/–	10 – 12 € pro User/✓

[1] Dienstleistungen: a Produkt- b Anwender- c Administratorenschulung, d Einführungs-, e Prozess-, f Integrationsberatung, g weitere [2] ISO-Länderkennung [3] nur über Drittanbieter
[4] über Konnektor [5] Datenarten: a Nutzerkonten, b Benutzereinstellungen, c Nutzergruppen, d E-Mails, e E-Mail-Verteiler, f Adressen, g Termine, h Aufgaben, i gemeinsame Ordner, j Notizen
[6] GF – Grundfunktionen: Adressen/Kontakte, Aufgaben, E-Mail, gemeinsame Folder, Kalender, Notizen [7] erweiterte Funktionen: a Projektmanagement, b Dokumentenverwaltung, c Helpdesk, d Workflow, e CRM, f Volltextsuche, g CTI-Anbindung, h Portalfunktion, i Shared Workplace, j Foren, k Usenet, l Instant Messaging, m Wiki, n Wissensdatenbank, o Umfragesystem, p Intranetportal

teamXchange 2.1.1	Kolab für UCS 2.0	WICE CRM-Groupware 5.2	Zarafa 6.0
VIPcom GmbH	Univention GmbH	WICE GmbH	Zarafa Deutschland GmbH
info@vipcomag.de	info@univention.de	info@wice.de	info@zarafaserver.de
www.vipcomag.de	www.univention.de	www.wice.de	www.zarafaserver.de
4800	100 000 User	4000	3000
a – f	a – f	a – f	a – f
DE, EN, FR, weitere/DE, EN/DE, EN	DE, EN, FR, weitere/DE, EN/DE	DE, EN/DE, EN/DE	DE, EN, FR, weitere/EN/DE, EN, FR, NL
Client/Server	Client/Server mit Fat Client und Webzugriff (AJAX)	Webanwendung (Perl) mit Browser-Zugriff	Client/Server mit Fat Client und Webzugriff (AJAX/gSOAP)
ab 98/✓/–/–/–/–	ab 2000/✓/–/✓/✓/✓	2000/–/–/✓/–/–	ab 2000/✓/–/–/✓/✓
–/Evolution, Kontact, Wilken OSBL (Open Source Business Library)	✓/Kontact, Sunbird	–/–	–/Evolution, Kontact, Thunderbird, Sunbird, Apple Mail, iCal, ...
k. A.	✓/E-Mail, Kalender, Kontakte, Aufgaben, Notizen, gemeinsame Folder, Terminplanung (Einladungen, free/busy)	✓/vollständig	✓/analog zu Outlook
Windows, Linux (x86, S/390)	Linux (Univention Corporate Server)	Linux	Linux
Windows, Linux	Windows, Linux, Unix mit KDE	Windows, Linux, Unix, Mac OS X	Windows, Linux, Unix, Mac OS X
1 GByte RAM	k. A.	k. A.	empfohlen: 4 GByte RAM, RAID1/RAID10
20 MByte	k. A.	k. A.	Outlook- bzw. Browser-Anforderungen
Client: DSL, 100 MBit/s	k. A.	k. A.	Clients: ab 9600 baud bzw. 56 KBit/s, 100 MBit/s
POP3, IMAP4, SMTP[Auth], LDAP[S], MAPI vollständig, andere	POP3[S], IMAP4[S], SMTP[Auth], TLS/SSL, LDAP[S], MAPI vollständig, andere	POP3[S], IMAP4[S], SMTP, TLS/SSL, LDAP	POP3[S], IMAP4[S], SMTP[Auth], TLS/SSL, LDAP[S], MAPI vollständig
CSV, TXT, LDIF, vCard, iCal, PST	CSV, TXT, LDIF, vCard, iCal, PST, E-Mail als MBox	CSV, XLS	CSV, TXT, LDIF, vCard, iCal, PST
CSV, TXT, LDIF, vCard, iCal, PST	CSV, TXT, LDIF, vCard, iCal, PST, E-Mail als MBox	CSV, vCard, iCal, XLS	CSV, TXT, LDIF, vCard, iCal, PST
AD, LDAP/k. A.	AD, LDAP/LDAP	LDAP/LDAP	AD, NT-DOM, LDAP, NIS[+], eDirectory/–
k. A.	–	–	AD, NT-DOM, LDAP
–	–	✓	–
–/Postfix, Exim, James	✓/–	✓/✓	–/✓
Fax, Voicemail, VoIP	– (nur über Client-Plug-Ins)	Fax, VoIP	Fax, VoIP, Videokonferenz
–/✓ (Wilken OSBL)/–	–/–/–	–/–/–	SugarCRM via Z-Merge/alle SOAP-basierten via Z-Merge/✓
1500/1500	> 50 000/< 2000 Fat Clients	keine Einschränkungen	2500/1000
–/–	✓/✓	–/✓	✓/✓
–/Outlook, (SyncML)[3]	✓/Outlook, Kontact, SyncML, KitchenSync	–/–	✓/Outlook, Activesync, Z-Push
k. A.	PalmOS, Windows Mobile, Symbian, Blackberry, alle SyncML-fähigen	–	Windows Mobile, Symbian
✓/✓	✓/✓	✓/–	✓/✓
–/–/✓	✓/✓/✓	–/–/✓	–/✓/–
✓/✓	✓/✓	–/✓	–/✓
✓/✓	✓/✓	–/✓	–/✓
–	✓, eigene Tools	✓, eigene Tools	✓, eigene Tools und Drittanbieter
✓/–/✓/–/–/–	✓/✓/✓/–/–/–	✓/–/✓/✓/✓/–	✓/✓/✓/–/✓/Cyrus IMAP, Maildir, Mbox, Tobit David
a, d, e, f, g, h, i	a, b, c, d, e, f, g, h, i, j	d, f	a, b, d, f, g, h, i
GF[6]	GF[6]	GF[6], a – g	GF[6], f (Volltextsuche)
proprietär/pro User	diverse Open-Source-Lizenzen, Konnektor proprietär/pro Server, User	eigene OSS-Lizenz/pro User	proprietär/pro User
0 €/20 – 60 €/0 €	220 €/14 €/0 €	0 €/0 €/450 €	150 €/30 €/0 €
18%/–	ab 4,90 € pro User/✓	18% der Lizenzkosten/–	20% vom Listenpreis/✓





Mäuserennen

Susanne Nolte

Je älter die IT wird, desto dichter drängen sich ihre Jubiläen. Nun dürfen die mausgesteuerten Desktop-Computer ihren 25-jährigen Geburtstag feiern.

Bis die ersten PCs mit grafischer Oberfläche 1983 ihren Weg in die Läden fanden, hatten Systeme mit „Zeigereingabegerät“ bereits einen langen Weg hinter sich. Nachdem Doug Engelbart 1963 die erste Maus entworfen hatte, eine Art Handwalze, die die Bewegungen in x- und y-Richtung auf den Bildschirm übertrug, arbeitete sein Team an multiplen Bildschirmfenstern (Windows). Die präsentierten sie 1968 erstmals der Öffentlichkeit.

Weitere fünf Jahre später zeigte das Xerox Palo Alto Research Center (PARC) den Prototyp eines Groß-Computers namens Xerox Alto mit GUI und Maus. Er kam zwar 1978 in die Läden, verkaufte sich aber nur an Universitäten – immerhin kostete er 32 000 US-$.

Doch auch der 1981 vorgestellte und mit 16 500 US-$ ebenfalls nicht preiswerte Nachfolger namens Star verkaufte sich nicht; ebenso wenig wie das etwa 6300 US-$ teure Xerox System 6085, das 1985 bereits über eine optische Maus verfügte und die Ära der PARC-Computer abschloss. Ihren Platz in der Ahnengalerie haben sich die PARC-Rechner vor allem als Vorbilder für zwei erfolgreiche und vor allem langlebige Desktop-Familien verdient: Microsoft Windows und Apple Macintosh.

Denn Steve Jobs begann 1979 mit der Entwicklung eines Systems, das die nächste PC-Generation begründete. Es sollte auf einem 16-Bit-Prozessor basieren, mit seiner Oberfläche neue Maßstäbe setzen und dabei nur 2000 Dollar kosten. Dafür suchte Jobs einen Partner und wurde fündig: Xerox investierte eine Million Dollar in Apple-Aktien, und Jobs erhielt mit seinem Lisa-Team Einblick ins PARC. Bei den Bemühungen, das Xerox-Konzept auf die Lisa zu übertragen, verlor das Team allerdings den Kostenaspekt völlig aus den Augen: Entgegen den ursprünglichen Plänen erhielt Lisa nun eine Maus und einem Monitor mit schwarz-weißer Bildröhre statt des grün-schwarzen Bildschirms.

Doch erst im Mai 1983 lieferte Apple die erste Lisa aus – mit dem neuen, 5 MHz schnellen Motorola 68000, 512 oder 1024 KByte RAM, 32 KByte Video-RAM, einer 5-MByte-Platte, zwei 5 1/4"-Floppy-Laufwerken, einem 12"-Schwarz-Weiß-Monitor mit 720 × 360 Pixeln, zwei DB25-Ports, einem Centronics-Port und drei internen Slots; Preis: etwa 10 000 US-Dollar.

Die Konkurrenz, die auch dieses System zum Ladenhüter werden ließ, kam aus dem eigenen Haus: Denn ausgerechnet bei der ersten Präsentation von Lisa im Januar 1983 berichtete Jobs vom nächsten System „Macintosh“, das über alle Fähigkeiten der Lisa verfügen, aber nur 2000 Dollar kosten sollte. Konsequenterweise taufte Apple die im Januar 1984 ausgelieferte Lisa II 1985 in Macintosh XL um. Nachdem bis 1986 insgesamt 100 000 Lisas verkauft waren, ließ Apple die letzten 2700 auf einem Acker in Utah unterpflügen, um sie von der Steuer abzuschreiben.

Als Apple die Lisa bereits ein halbes Jahr lang auslieferte, kündigte Microsoft einen schlanken DOS-Aufsatz an: „Microsoft Windows essentially treats the computer screen as a ‚desk-top’ with application windows neatly arranged in logical fashion.“ Dabei verschwieg Microsoft auch nicht die Anleihe beim Xerox Star: „Microsoft Windows is an outgrowth of a concept that was originally developed by Xerox for use on the Star.“ Doch auch diese Oberfläche hatte ihre Anlaufschwierigkeiten: Statt Anfang 1984 kam Windows erst im November 1985 auf den Markt. Bis zur Version 3.0 war es ein reines Verlustgeschäft.

Totgesagte leben länger

Ebenfalls im Mai 1983 begann IBM zusammen mit Microsoft, OS/2 unter dem Motto „Better DOS than DOS“ zu entwickeln. Wirklich eingelöst und gleichzeitig verworfen hat Big Blue das Versprechen knapp zehn Jahre später: 1992 hatte die von IBM allein weiterentwickelte 32-Bit-Version OS/2 2.0 nichts mehr mit DOS zu tun. Obwohl der Verkauf seit 23. 12. 2005 und der Support seit 31. 12. 2006 eingestellt ist, verkauft IBM noch heute in Ausnahmefällen Lizenzen für Spezialanwendungen. Dass der 25. Geburtstag dennoch keine Trauerveranstaltung wird, ist der Firma Serenity Systems zu verdanken. Sie lizenzierte 2000 OS/2, entwickelt es seit 2002 weiter und vertreibt es heute noch unter der Bezeichnung eComstation (ecomstation.com).

Das jenseits der Microsoft-Welt wohl wichtigste Fenstersystem ist das X Window System, das gerade einmal ein Jahr nach Lisa das Licht der Welt erblickte: 1984 gründeten das MIT, DEC und IBM das Projekt Athena und gaben im Juni die erste X-Version frei. Die erste Release der heute noch aktuellen Version X11 folgte 1987. Zehn Jahre später mauserte sich die freie Implementierung XFree86 zum De-facto-Standard. Heute entwickelt die X.Org-Foundation sie weiter. (sun)



Sinn und Unsinn zentraler Verschlüsselungslösungen

Schlüsselfreiheit

Christoph Wegener

Die vertrauliche Übermittlung von Daten und der Nachweis der Urheberschaft rücken bei digitalen Kommunikationsmethoden wie E-Mail immer stärker in den Vordergrund. Viele liebäugeln mit zentralen Lösungen zur Integration der benötigten Verschlüsselungsverfahren, die das Nutzen von Verfahren wie PGP und S/MIME vereinfachen sollen.

Wenngleich E-Mail den Spam-Massen zum Trotz ständig an Beliebtheit gewinnt, verläuft geschäftliche Kommunikation häufig nach wie vor auf dem klassischen Postweg. Als Hauptgrund hierfür nennen die Unternehmen, dass die Vertraulichkeit der Informationen so sichergestellt sei. Viel lieber würden sie die geschäftliche Kommunikation gänzlich auf elektronischem Wege abwickeln, denn das geht schnell, unkompliziert und spart vor allem Geld.

Doch alte und neue Regularien wie der Sarbanes-Oxley Act (SOX), das Gesetz zur Kontrolle und Transparenz (KonTraG), aber auch das Aktiengesetz (AktG) oder das Bundesdatenschutzgesetz (BDSG) beschreiben Anforderungen an die Sicherheit der Unternehmenskommunikation, die den Einsatz von E-Mails im Klartext in vielen Fällen verbieten. Trotzdem erkennen längst nicht alle Unternehmen die Risiken der Kommunikation per unverschlüsselter E-Mail.

Ein wesentliches Kennzeichen von asymmetrischen Verschlüsselungsverfahren wie PGP ist die Existenz eines Schlüsselpaares, das aus einem privaten und einem öffentlichen Schlüssel besteht. Der private, geheime Schlüssel dient einerseits zum Entschlüsseln verschlüsselter Daten, andererseits zum Erstellen von Signaturen. Der öffentliche Schlüssel hingegen kommt für das Verschlüsseln von Daten und das Überprüfen von Signaturen zum Einsatz. Der private Schlüssel darf – wie der Name nahelegt – nur dem Besitzer zugänglich sein. Um das sicherzustellen, ist er in der Regel mit einem Passwort vor unbefugtem Zugriff geschützt.

Trau keinem Dritten

Dieses Verfahren führt allerdings in der Praxis zu einem erheblichen Aufwand: Woher weiß der Absender einer verschlüsselten E-Mail oder der Empfänger einer signierten E-Mail, dass der öffentliche Schlüssel, den er verwendet, wirklich dem eigentlichen Empfänger oder Absender der E-Mail gehört und nicht einem Unbefugten?

Hier macht man sich zunutze, dass sich die verwendeten öffentlichen Schlüssel auch signieren lassen – was allerdings erst geschehen darf, nachdem sich der Signierende auch von der Identität desjenigen überzeugt hat, der den Schlüssel ausgibt. Auf diese Weise lassen sich im Prinzip regelrechte

Vertrauensketten erstellen (Web of Trust). Wenn im Web of Trust nur ein Beteiligter zu nachlässig ist, fällt das Konstrukt jedoch in sich zusammen, wogegen es keinen einfachen Schutz gibt.

Darüber hinaus ist auch das Verwalten der Schlüssel nicht trivial, beispielsweise für den Fall, dass der private Schlüssel eines Benutzers in falsche Hände gerät. Sollte es überhaupt auffallen, steht der Eigentümer vor der Aufgabe, alle Kommunikationspartner über den Sachverhalt zu informieren, bevor Dritte Schaden anrichten können. Natürlich gibt es Verfahren, einen Schlüssel zurückzurufen, die aber leider nicht konsequent umgesetzt sind.

Von Authentifizieren bis Zertifikat

Neben PGP und verwandten Verfahren lassen sich digitale Zertifikate zur Sicherung der Kommunikation in puncto Vertraulichkeit und Integrität nutzen. Auch digitale Zertifikate beruhen allerdings auf asymmetrischer Kryptografie mit privaten und öffentlichen Schlüsseln. Der Unterschied gegenüber Technologien wie PGP besteht darin, dass ein digitales Zertifikat die Authentizität einer Person bestätigen kann. Dazu existiert eine vertrauenswürdige Instanz, die sogenannte „Certification Authority“ (CA), die das Zertifikat erst dann ausstellt und digital signiert, wenn eine als „Registration Authority“ (RA) bezeichnete Stelle (die häufig mit der CA vereint ist) die Authentizität des Beantragenden anhand von eindeutigen Merkmalen bestätigt hat.

In der Praxis scheitert es jedoch oft schon am Prüfen dieser eindeutigen Merkmale. Zum Ausstellen von SSL-Zertifikaten reicht häufig gar die Angabe einer E-Mail-Adresse und einer Telefonnummer, die dann per automatisiertem Rückruf die Identität des E-Mail-Empfängers sicherstellen soll. Sinnvoller und eigentlich auch erforderlich wäre das persönliche Erscheinen des Antragstellers und die Bestätigung seiner Identität und Legitimation durch Vorlegen offizieller Dokumente (etwa Personalausweis oder Reisepass) mit Foto.

Das Verwalten der Zertifikate birgt prinzipiell die gleichen Tücken wie die asymmetrische Verschlüsselung: Auch hier gibt es eine sogenannte „Certificate Revocation List“ (CRL), deren konsequente Anwendung aber leider noch nicht gängige Praxis ist. Somit ist die Beurteilung der Integrität eines Zertifikats für den normalen Anwender eine nicht einfach zu lösende Aufgabe.

Erleichterung versprechen Verfahren, die einen zentralen Ansatz nutzen, der den beschriebenen Komplikationen der Verwaltung und Integrität der Schlüssel und Zertifikate begegnet. Sie verlagern den Vorgang der Ver- und Entschlüsselung zumeist auf ein Gateway, etwa das Mail-Gateway des Absenders. Dann müssen sich die Anwender nicht mehr einzeln um die Verwaltung der Schlüssel oder Zertifikate kümmern, denn diese Aufgabe erledigt das System oder ein Administrator zentral. Ob eine E-Mail verschlüsselt werden soll, lässt sich in zentralen Regelsätzen auf Basis von Betreffzeile, Inhalt, Empfänger oder Absender ermitteln. Einige Systeme bieten dem Anwender zudem zusätzlich die Möglichkeit einer Ende-zu-Ende-Verschlüsselung.

Die Vorteile solcher Lösungen liegen auf der Hand: Sie entlasten den Anwender weitgehend von der Komplexität, die die Integration von Verschlüsselungsverfahren nicht nur im E-Mail-Verkehr so langwierig, kostspielig und auch fehleranfällig macht. Diese Aufgabe übernimmt nun der Administrator, der mit hoher Wahrscheinlichkeit den entsprechenden Sachverstand zur Lösung der diversen Probleme besitzt. Aufgrund des zentralistischen Ansatzes lassen sich auch Vorgaben, wann Daten zu verschlüsseln oder zu signieren sind, wesentlich einfacher umsetzen. Damit sind entsprechende Vorgaben nicht nur einfacher, sondern oft überhaupt erst nachweisbar zu erfüllen. Manchmal genügt es, dass eine Signatur nur die absendende Organisation, nicht aber die absendende Person nachweist. Das funktioniert mit ein wenig Technik auch ohne wesentliche Einschränkungen bezüglich der Sicherheit mit einem zentral gestalteten Ansatz.

Nicht besonders geheim

Darüber hinaus reduzieren zentrale Systeme den Aufwand für das Verteilen und Konfigurieren von Client-Software auf die Anwender-PCs erheblich, wenngleich sie für Verfahren mit Ende-zu-Ende-Verschlüsselung weiterhin nötig ist. Entsprechende Ansätze, die einfache Browser-Plug-ins nutzen, vereinfachen den Vorgang weiter. Je nach Produkt kann der Nutzer per Browser seine Schlüssel erstellen und verwalten – was die grundsätzlichen Schwächen aber nicht behebt.

Zum einen verletzen zentrale Systeme das Prinzip, den privaten Schlüssel unbedingt geheim zu halten, in eklatanter Art und Weise, denn letztlich hat der Administrator des E-Mail-Gateways Zugriff darauf. Somit kann er – falls der Nutzer nicht zusätzlich eine Ende-zu-Ende-Verschlüsselung einsetzt – verschlüsselte E-Mails mit vertraulichem Inhalt unbemerkt entschlüsseln, falls hier nicht gesonderte Vorkehrungen getroffen werden. Zudem erweist man den Anwendern aus Sicht der „Awareness“ eventuell einen Bärendienst: Es stellt sich nämlich die Frage, wie man Nutzer zu einem vorsichtigen Umgang mit „geheim“ zu haltenden Daten (etwa Passwörtern und Zugangsschlüsseln) erziehen will, wenn man auf der anderen Seite ein Verfahren etabliert, in dem die „privaten“ Schlüssel gar nicht geheim sind.

Zum anderen obliegt das Sicherstellen von Authentizität und Integrität der Schlüssel nun einem Administrator. Das kann ein Vorteil sein, da es einen geregelten Prozess gibt, der das Überprüfen von Schlüsseln vereinfacht. Jedoch steigt der administrative Aufwand bei einer Vielzahl von Kommunikationspartnern erheblich. Hier können Public-Key-Infrastrukturen auf Zertifikatsbasis helfen, da der Administrator dann „nur“ die Gültigkeit des Zertifikates überprüfen muss. Genau das birgt aber mögliche Fallstricke, denn gerade bei vielen Kommunikationspartnern in verschiedenen Institutionen ist es derzeit nicht immer einfach, den Fingerabdruck der Zertifikate auf vertrauenswürdigem, unabhängigem Wege zu bekommen.

Einige Lösungen speichern die Schlüsselpaare zudem sogar auf einem Server, der nicht einmal im direkten Zugriffsbereich des Anwenders oder seines Administrators steht, sondern der von einem Dritten gehostet wird. So ist die Integrität der Schlüssel nicht mehr gegeben, und es stellt sich die Frage, was denn mit verschlüsselten Daten oder E-Mails passieren soll, wenn der Hoster dieses Servers einmal pleite geht. Wie kommt man dann noch an seine Daten? Wer bekommt in einem solchen Fall Zugriff auf die Schlüsselpaare? Gerade Unternehmen, aber auch Privatpersonen sollten sehr vorsichtig sein, ob und wie sie einen solchen Service nutzen wollen. Zumindest ein auf anderem Wege verschlüsseltes, unabhängiges Backup der Daten empfiehlt sich, will man etwa erpresserischen Debatten aus dem Wege gehen.

Außerdem kann ein Administrator oder generell derjenige, in dessen Zugriff sich der private Schlüssel befindet, auch im Namen des Nutzers signierte E-Mails verschicken – was mit erheblichen Konsequenzen verbunden sein kann. Das Abstreiten einer signierten E-Mail wird dem Betrogenen in aller Regel Schwierigkeiten bereiten, wenngleich die Sensibilisierung und das Verständnis der Gerichte für den Ablauf solcher Betrugsfälle in letzter Zeit – auch durch Trojaner im Onlinebanking – gestiegen sind.

Gegen das Argument, der Administrator habe eben einfach vertrauenswürdig zu sein, spricht schon die Statistik. Sie zeigt immer wieder, dass gerade Insider einen erheblichen Teil der Angriffe verüben. Besser wäre es in jedem Fall, entsprechende Sicherungs- und Protokollierungsmaßnahmen einzuführen, die den Anwender vor dem Missbrauch seiner Schlüssel schützen. Wie dies im Falle von gehosteten Angeboten realisiert werden soll, bleibt offen. Anwender sollten sich stets bewusst sein, dass es eine hundertprozentige Sicherheit nicht geben kann.

Fazit

Zentrale Lösungen zum Ver- und Entschlüsseln von E-Mails bieten eine Reihe von Vorteilen. Sowohl für Anwender als auch für Administratoren erleichtern sie die Einführung und den Support. Zudem lassen sich Grundregeln zur Verschlüsselung – auch für hartnäckige Krypto-Ignoranten unter den Anwendern – einfacher umsetzen, wenn es einen zentralen Punkt der Kontrolle gibt. Besser als gar nichts, könnte man denken, wirklich geheime Daten schützen derlei Verfahren allein aber nicht, denn gegen Innentäter sind sie wirkungslos. Wer denen einen Riegel vorschieben will, kommt um eine deutlich aufwendigere Ende-zu-Ende-Verschlüsselung nicht herum. Mit einer zentralen Signaturlösung ist zudem unter Umständen eine Reihe von Risiken verbunden, derer man sich bei der Integration in die Geschäftsprozesse bewusst sein sollte. (un)

CHRISTOPH WEGENER

ist Certified Information Systems Auditor (CISA), promovierter Physiker und seit 1999 mit der wecon.it-consulting freiberuflich in den Bereichen IT-Sicherheit und Open Source/Linux aktiv.

Onlinequellen

RFCs	www.rfc.net
Universal Gateway Email von PGP	www.pgp.com/de/
Ironports Appliance Post-X	www.ironport.com/de/
Astaros Security Gateway	www.astaro.de
Reddoxx Mailsealer	www.reddoxx.com/mailsealer.html
Freenigma	www.freenigma.com
Securemail Gateway von Voltage	www.voltage.com

Produktlinien in der industriellen Softwareentwicklung

Gleichheit in Vielfalt



Klaus Schmid

Software ist ein entscheidender Wertschöpfungs- und Kostenfaktor in industriellen Produkten. Dies gilt sowohl für Informationssysteme als auch für eingebettete Systeme wie Anlagensteuerungen oder Automobilkomponenten. Systematische Produktlinienentwicklung hat sich als probates Mittel erwiesen, gleichzeitig Kosten und Fehlerzahl zu senken.

Im Verlauf der letzten zehn, fünfzehn Jahre hat sich der Einsatz von Produktlinienansätzen als wirksame Methode herauskristallisiert, um Optimierungen bezüglich Kosten und Qualität bei der industriellen Softwareentwicklung zu erreichen. Die dabei erzielten Erfolge sind beachtlich. So berichten verschiedene Unternehmen von Kostenreduktionen um 90 %, einer deutlich erhöhten Qualität (circa 50 % weniger Fehler) sowie drastisch reduzierten Wartungskosten [2].

Begründet ist dies zum einen durch den Übergang von der Entwicklung einzelner Anwendungen zu einer gemeinsamen Betrachtung einer Menge von Systemen, zum anderen durch die Entwicklung von Komponenten, die in einer Vielzahl von Systemen verwendet werden können. Damit ist aber zugleich eine wesentliche Einschränkung dieses Ansatzes gegeben: Er ist nur anwendbar, wenn eine Entwicklungsorganisation immer wieder ähnliche Software entwickelt. Bei näherem Hinsehen ist dies aber keine wesentliche Einschränkung, da Entwicklungsabteilungen und Firmen praktisch immer auf die eine oder andere Art spezialisiert sind.

Unter dieser Voraussetzung hat sich der Produktlinienansatz als zielführend erwiesen. Er kam sowohl in kleinen als auch in großen Unternehmen zum Einsatz, bei Entwicklermannschaften zwischen fünf und mehr als tausend Personen. Auch in diversen Anwendungsbereichen wurde er bereits umgesetzt, das Spektrum reicht von der Automobilindustrie und Medizintechnik bis hin zu Finanzinformationssystemen [3].

Grundlagen der Produktlinien

Dabei unterscheidet sich Produktlinienentwicklung von den – meist wenig erfolgreichen – Ansätzen zur Softwarewiederverwendung in einigen wichtigen Punkten.

Ausgehend von einigen Einzelfällen – vor allem aus den frühen 90ern – wurde im Verlauf der letzten zehn Jahre systematisch herausgearbeitet, was bei der Produktlinienentwicklung wichtig ist. Es gibt kleine Unterschiede in der Darstellung, doch letztendlich kann man sie wie folgt zusammenfassen:

Geschäftsorientierung: Die Entwicklung der Produktlinie ist wesentlich durch die Geschäftsstrategie des Unternehmens und die vom Unternehmen konkret zu entwickelnden Produkte getrieben.

Variantenmanagement: Der Übergang von einer Einzelsystemsicht auf eine übergreifende Produktliniensicht rückt die Unterschiede zwischen Systemen in den Mittelpunkt.

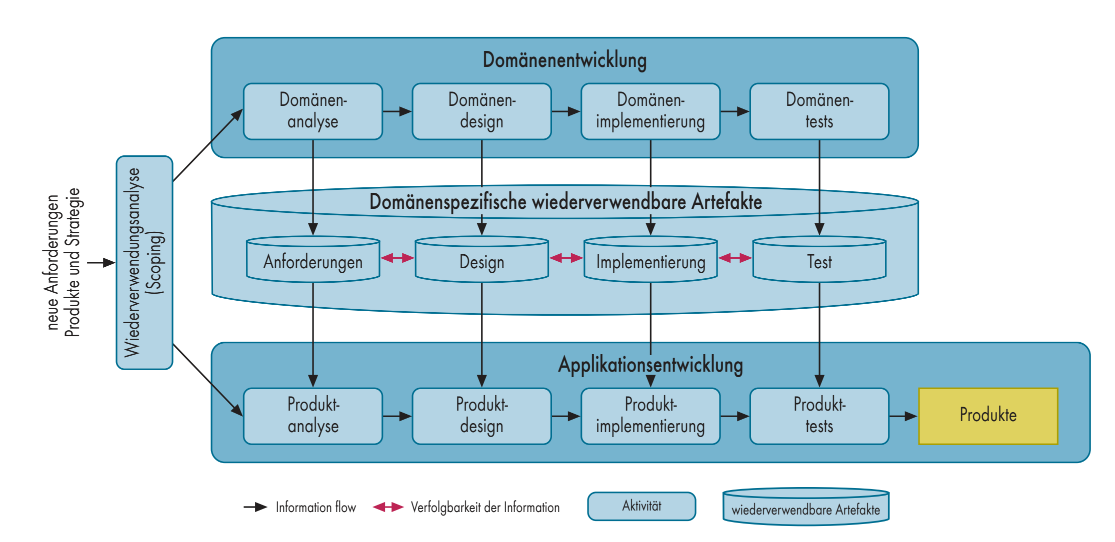
Architekturzentrierte Entwicklung: Die technische Basis ist zwar nicht die einzige, aber eine sehr wichtige Grundlage für eine Produktlinienentwicklung. Dabei geht es insbesondere darum, eine einheitliche Architektur und Plattform zu schaffen, die für die aktuellen wie für die zukünf-

tigen Produkte eine geeignete Basis bildet.

Produkt- vs. Produktlinienentwicklung: Eine klare konzeptionelle Trennung zwischen der Entwicklung von Komponenten, die für die Wiederverwendung über eine Menge von Produkten hinweg bestimmt sind, und der von Einzelprodukten. (Dies ist nicht immer, aber oft mit einer organisatorischen Trennung verbunden.)

Damit ergibt sich, dass Produktlinienentwicklung ein notwendig ganzheitlicher Entwicklungsansatz ist: Das Verfahren betrifft technische, methodische und organisatorische Aspekte ebenso wie die Geschäftsstrategie des Unternehmens. Rein technikgetriebene Ansätze sind hingegen selten erfolgreich.

Prinzipiell werden bei der Produktlinienentwicklung zwei verschiedene Lebenszyklen unterschieden: die Applikationsentwicklung, verantwortlich für die Erstellung der eigentlichen Produkte, und die Domänenentwicklung, zuständig für den Bau der wiederverwendbaren Artefakte. Auf dieser Basis werden anschließend im Rahmen der Applikationsentwicklung die einzelnen Produkte entwickelt (siehe Abbildung 1).



Die Produktlinienentwicklung besteht aus zwei verschiedenen Prozessen: der Domänenentwicklung und der Applikationsentwicklung (Abb. 1).

Am Anfang steht das Scoping

Meist ist auch mithilfe der wiederverwendbaren Artefakte noch die Entwicklung zusätzlicher Produktbestandteile als Spezialanfertigung notwendig. Es müssen dabei nicht alle wiederverwendbaren Artefakte zwingend in allen Produkten genutzt werden, sondern sie sind relativ frei integrierbar – quasi Plug and Play auf Softwareebene.

Das sogenannte Scoping, die Planung, welche Bestandteile wiederverwendbar zu implementieren sind und welche nicht, ist ein wesentlicher Bestandteil der Entwicklung. Entscheidend ist, tunlichst nur solche Funktionen wiederverwendbar zu machen, die später auch noch einmal zum Einsatz kommen. Denn sonst steckt man unnötige Investitionen in die Wiederverwendung. Andererseits muss man das vorhandene Wiederverwendungspotenzial ausnutzen, um einen möglichst hohen Return on Investment (ROI) zu erzielen. Das dafür verantwortliche Management muss übergreifend die gesamte Produktlinie im Blick haben und dabei die Anforderungen, die in die Applikationsentwicklung einfließen, von solchen abgrenzen, die direkt in die Domänenentwicklung eingehen. Dieser Prozess muss auch kontinuierlich im Falle von Anforderungsänderungen oder neuen Produkten durchgeführt werden.

Was die konkreten Resultate einer Produktlinie angeht, gibt es mittlerweile sehr viele gut dokumentierte, auch prominente Beispiele [3]. Eines ist die Produktlinie „i* ProductLine“ der Market Maker Software AG. Die Software gibt es in einer Vielzahl von Varianten. Zwei Beispiele sind Arbeitsplatzsysteme für einen Wertpapierberater in einer Bank und als Spezialsystem für Metallhändler (siehe Abbildung 2 und 3). In dieser Produktlinie sind sehr große Gemeinsamkeiten in der Implementierung der Funktionsbestandteile vorhanden, jedoch sind die Oberflächen deutlich verschieden.

Ein weiteres Beispiel für eine Produktlinie liegt mit dem Warenwirtschaftssystem der Firma Maxess Systemhaus GmbG vor. Auch diese gibt es in einer Vielzahl von Varianten. Die Überlappungen zwischen den beiden Anwendungen erstrecken sich über alle Bereiche bis hinein in die Benutzeroberfläche, wie Screenshots der Auftragserfassung am Beispiel der Varianten für den Lebensmittelhandel und den technischen Handel zeigen (Abb. 4 und 5).

iX-TRACT

- In der industriellen Softwareproduktion wurde durch Produktlinienentwicklung nicht nur Zeit gespart, sondern auch die Qualität verbessert.
- Das A und O der Produktlinienentwicklung ist das systematische Management von Unterschieden zwischen Produkten (Variantenmanagement) über die komplette Entwicklung hinweg.
- Die Entwicklung wiederverwendbarer Komponenten in der Produktlinienentwicklung ist eng mit der Unternehmensstrategie verzahnt.

Wiederverwendung als Basis

Produktlinienentwicklung basiert letztendlich auf der Grundidee der Softwarewiederverwendung. Oder genauer: der Softwareverwendung über eine Menge von Produkten hinweg. Traditionelle Wiederverwendungsansätze beruhen entweder auf dem Versuch, Komponenten oder Dokumente aus früheren Projekten wiederzuverwenden oder darauf, abstrakt „generische“ Komponenten zu entwickeln. Im Gegensatz dazu werden in einer Produktlinie mehrfach verwendbare Komponenten zielgerichtet auf ein Produktportfolio unter vorhersehbaren technischen Rahmenbedingungen entwickelt.

Eine Grundlage dafür bildet die Produkt-Roadmap. Somit ist zunächst das Management gefordert, eine hinreichend ausformulierte Strategie beziehungsweise ein Produktportfolio zu definieren. Basierend darauf wird eine Domänenanalyse durchgeführt. Diese beschreibt nicht nur mögliche Produkte und Produktanforderungen, son-

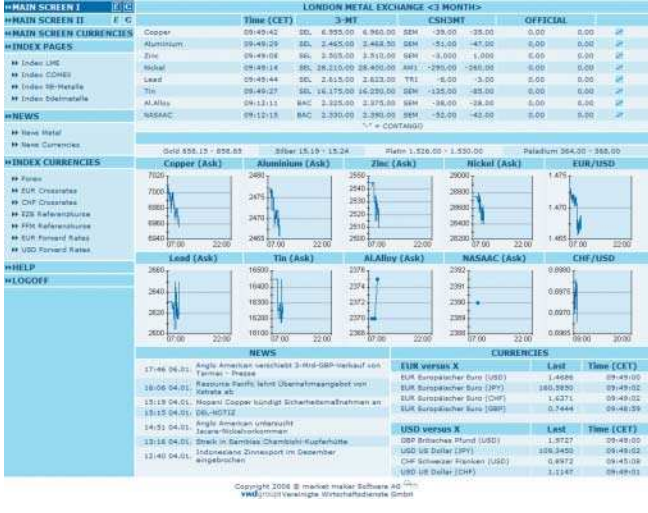
dern detailliert auch mögliche Unterschiede zwischen Produkten sowie Abhängigkeiten zwischen variablen Anforderungen.

Knackpunkt Varianten

Im Laufe der Zeit wird sich dieser Zeitplan natürlich verändern und weiterentwickeln, wichtig ist jedoch, eine konkrete Vision der Produkte und der notwendigen Variabilität zu entwickeln und kontinuierlich fortzuschreiben. Dies funktioniert nur, wenn man dafür entsprechende Rollen und Verantwortlichkeiten schafft. Dazu gehört insbesondere ein produktlinienweites Change Control Board (CCB), das für die Koordinierung und Einordnung von Änderungen über die Produktlinie hinweg verantwortlich ist. Insbesondere muss es entscheiden, welche Änderungen wiederverwendbar und welche produktspezifisch zu realisieren sind.

Der Übergang von der Entwicklung einzelner Systeme zu einer integrierten Entwicklung einer Reihe von Systemen führt zur Notwendigkeit des Variantenmanagements. Das heißt, es ist für die Entwicklung einer Produktlinie entscheidend, einen Überblick darüber zu haben,
– welche Anforderungen für alle Systeme gelten (Gemeinsamkeiten),
– welche Anforderungen nur für einen Teil der Produkte, aber nicht für alle relevant sind (Variabilitäten) und
– welche Anforderungen nur für bestimmte Produkte relevant sind (produktspezifische Anforderungen).





Verschiedene Varianten aus der gleichen Produktlinie von Online-Finanzinformationssystemen: oben Wertpapierberater, unten Metallhändler (Abb. 2, 3)

Neben den Anforderungen gilt dies prinzipiell für alle Arten von Entwicklungsartefakten. So ist beispielsweise in Bezug auf den Code relevant, welche Teile in allen, welche in manchen und welche nur in einigen wenigen Produkten benötigt werden.

Das Variantenmanagement hat einerseits eine organisatorische, andererseits eine technische Dimension. Organisatorisch ist vor allem wichtig, dass diese Analyse überhaupt stattfindet. Für Organisationen, die bereits Produkte entwickelt haben, bedeutet dies, innerhalb der Organisation einen kompletten Überblick über die Produkte, die von ihnen unterstützten Anforderungen sowie die damit zusammenhängenden Entwicklungsartefakte zu schaffen.

Für Organisationen, die neu mit einer Entwicklung starten wollen, ist dies insofern einfacher, als sie nur eine entsprechende Übersicht über die geplanten Produkte erstellen müssen.

Erfahrungsgemäß ist eine der größten Herausforderungen bei diesem Schritt, dass er überhaupt stattfindet. Meist wird er als unproduktiv empfunden, da er keinen direkten Mehrwert bringt. Jedoch ist er von wesentlicher Bedeutung für die weiteren Schritte. Gerade in kleinen Organisationen, in denen das Entwicklerteam die verschiedenen Produkte bereits gut kennt, ist die Illusion naheliegend, dieser Schritt sei überflüssig. Jedoch ist er auch dort notwendig, wenngleich wesentlich einfacher und weniger aufwendig.

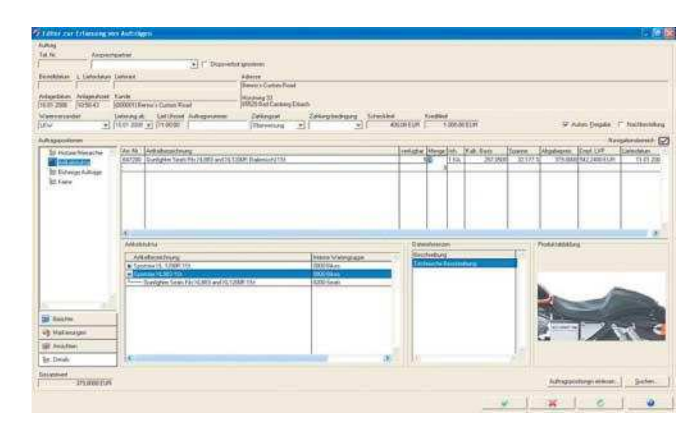
In der täglichen Entwicklungsarbeit ist wichtig, dass eine klare konzeptionelle Trennung von Entwicklung mit Wiederverwendung und Entwicklung für Wiederverwendung stattfindet. Das heißt nicht, dass verschiedene Personen oder gar Abteilungen dafür verantwortlich sind, sondern vielmehr, dass jeder Person, die in eine Entwicklung oder Änderung einbezogen ist, klar ist, ob es gerade um weitere Wiederverwendung geht oder um eine spezifische Produktentwicklung.

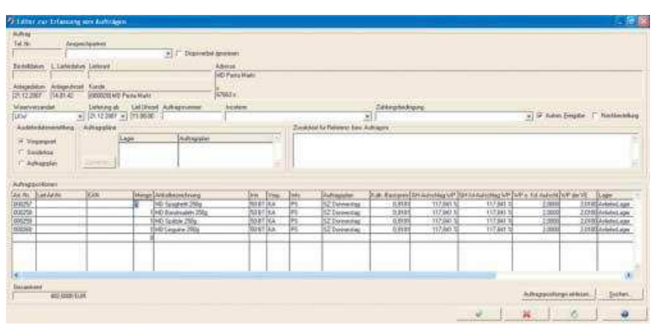
Mit oder für Wiederverwendung

Alle Informationen für wiederverwendbare Artefakte sollten in integrierter Weise dargestellt werden. Die Entwicklungsartefakte (etwa Anforderungen) für ein spezifisches System werden damit zu einer Projektion des allgemeinen Entwicklungsartefakts. Ein Problem ist jedoch, dass marktgängige Software-Entwicklungswerkzeuge die Variantenmodellierung bisher kaum unterstützen. Es gibt zurzeit nur einige wenige Hersteller, die Werkzeuge für das Variantenmanagement zur Verfügung stellen (siehe Textkasten „Werkzeuge“).

So verwenden die meisten Unternehmen zurzeit einfache Ersatzlösungen, die jedoch ausreichend sein können, zumindest für wenige Varianten oder eine kleine Entwicklungsmannschaft. Meist werden die etablierte Werkzeuge in spezifisch angepasster Weise oder selbstentwickelte Werkzeuganpassungen genutzt.

Der Kern des Variantenmanagements ist immer der Gleiche: ein Entwicklungsartefakt wird in seine Bestandteile zerlegt, die Gemeinsamkeiten, Variabilitäten und produktspezifische Aspekte darstellen. Dazu gibt es eine Beschreibung, welche Variabilitäten und welche produktspezifischen Bestandteile für jedes Produkt relevant sind. Konkrete Ausprägungen von Variantenbildungsansätzen können sich deutlich voneinander unterscheiden, abhängig vor allem von der Größe der Entwicklungsteams, der Zahl der zu unterstützenden Produkte sowie Restriktionen der verwendeten Werkzeuge. Insbesondere ist bei einer großen Zahl von Produkten eine Trennung der produktspezifischen Anteile und der Beschreibung der Produktrelevanz





Verschiedene Varianten aus der Auftragserfassung: oben technischer Handel, unten Lebensmittelhandel (Abb. 4, 5)

von den eigentlich wiederverwendbaren Anteilen von Bedeutung.

Wichtig beim Variantenmanagement ist vor allem, dass die Variation auf grundlegende Konzepte zurückgeführt wird und nicht nur auf bestimmte Kunden oder Aufträge. Bei der erwähnten Unterscheidung zwischen technischem und Lebensmittelhandel etwa war es wichtig, die Trennung an der Branche – und damit zusammenhängenden Entscheidungen – festzumachen (beispielsweise werden im Editor für den technischen Handel ein Vorschaubild und weitere Erläuterungen gezeigt) und nicht an den spezifischen Ausprägungen (Produkt für die XYZ-Auto GmbH).

Dies ist auch der zentrale Unterschied zu klassischen Ansätzen zur Entwicklung „generischer“ Komponenten: Eine Verallgemeinerung wird nur eingeführt, wenn die Produkte sie tatsächlich benötigen oder wenn sie sich aufgrund der strategischen Produktplanung ergibt. Dies vermeidet, dass Aufwand auf Verallgemeinerungen verschwendet wird, die man nie benötigt – ein Aspekt, der entscheidend für das Return on Investment einer Produktlinienentwicklung ist. (Die klassischen Prinzipien modularer Entwicklung sollten natürlich nach wie vor berücksichtigt werden.)

Nicht ziellos entwickeln

Im Rahmen einer Produktlinienentwicklung erfährt die Beschreibung der Softwareentwicklung durch Dokumente beziehungsweise Modelle eine Erweiterung gegenüber den Einzelsystemen. Hinzu kommt als Grundlage des Variabilitätsmanagements eine Variantenbeschreibung der Produktlinie. Dafür wurden verschiedene Ansätze entwickelt.

Der vielleicht einfachste und bekannteste Ansatz ist die sogenannte Featuremodellierung, die Beschreibung der wesentlichen Eigenschaften von Systemen durch Features. Die Definition neuer Systeme geschieht dann durch Auswahl der entsprechenden Features.

Eine etwas andere Sichtweise wird bei der Entscheidungsmodellierung (decision modelling) eingenommen. Hier stehen die wesentlichen Entscheidungen im Mittelpunkt, die im Rahmen der Produktentwicklung zu treffen sind, um von der allgemeinen Produktlinie zu den spezifischen Produkten zu kommen.

Oben war die Produktlinie der Finanzinformationssysteme erwähnt. Um diese hier als Beispiel verwenden zu können, muss sie allerdings drastisch vereinfacht werden. Ein stark vereinfachtes Modell stellt die Tabelle unten dar. Nur die wesentlichen Entscheidungen sind aufgeführt (hier nur ausgewählte Beispiele), um die jeweiligen Produkte zu definieren.

So werden im Metallgeschäft Forward-Kurse (Kurse für einen Verkauf in der Zukunft) genutzt, andererseits spielen beispielsweise bei Aktien verschiedene Daten wie Unternehmenskennzahlen oder Analysten-Ratings eine Rolle. Im Falle eines Fonds ist es beispielsweise hilfreich, seine Struktur in Form eines Diagramms darzustellen. Ein Entscheidungsmodell, wie stark vereinfacht in der Tabelle dargestellt, fasst nun diese Aspekte zusammen.

Referenzarchitekturen

Ein weiteres Prinzip der Produktlinienentwicklung ist die Architekturzentrierung. Eine Softwarearchitektur legt die Struktur eines Softwaresystems und damit seine Komponenten sowie deren Zusammenspiel fest. Bekannte Beispiele für eine Softwarearchitektur sind etwa die Client-Server- oder die Schichtenarchitektur. Eine Beschreibung wie „Client-Server“ reicht jedoch nicht, meist sind ein bis zwei weitere Detaillierungsebenen für eine hinreichende Beschreibung nötig.

Warum ist gerade die Architektur so wichtig für eine Produktlinie, viel wichtiger noch als für ein Einzelsystem? Ein Blick darauf, wie unterschiedlich die Variabilität einer Produktlinie auf eine Architektur abgebildet werden kann, erklärt den Zusammenhang.

Der einfachste Fall ist, dass prinzipiell ähnliche Funktionen

Entscheidungstabelle

Entscheidung	Relevanz	Wertebereich	Abhängigkeiten
Forwardkurse	Kurstabellen = True	1-Monat, 3-Monat, 6-Monat	–
Unternehmenskennzahlen	–	Cashflow, GuV, Bilanz, Segmente	Forward ≠ { } => Unternehmenskennzahlen = { }
währungsbereinigte Preise	–	True, False	–
Fondsstrukturdiagramm	Fonds in Wertpapierarten	True, False	–

Entscheidung benennt die Entscheidung (kann wie eine Variablendeklaration gelesen werden).

Relevanz beschreibt, ob die jeweilige Entscheidung überhaupt für ein Produkt sinnvoll ist. So ist ein Fondsstrukturdiagramm nur dann möglich, wenn überhaupt Fonds als Wertpapierart aufgeführt sind. (Dabei ist Wertpapierart eine weitere, nicht aufgeführte Entscheidung.)

Wertebereich gibt an, welche möglichen Werte die Entscheidung annehmen kann. Dabei kann eine Entscheidung auch eine Menge von Werten annehmen, beispielsweise ist „Unternehmenskennzahlen = {Cashflow, GuV}“ möglich.

Abhängigkeiten beschreiben Zusammenhänge zwischen den Werten der einzelnen Variablen. Die Definition dieser Entscheidungen kann dann wiederum genutzt werden, um die Variation in verschiedenen Softwareentwicklungsartefakten (beispielsweise Anforderungsdokumente) geeignet zu beschreiben.

auf verschiedene Weisen realisiert werden können. Man denke hier beispielsweise an Komponenten zum Benutzermanagement, die technisch durch verschiedene Alternativen umgesetzt sein können (etwa LDAP vs. lokal).

Dies kann man architektonisch durch den Austausch von Komponenten erreichen, muss dann aber sicherstellen, dass die Komponenten sich gegenüber dem Rest des Systems weitgehend identisch verhalten. Dies wiederum erfordert ein genaues Verständnis (und eine Festlegung) des Zusammenspiels zwischen Architektur und Umgebung. Da die Produktlinienarchitektur in diesem Sinne nicht fix ist wie die Architektur eines Einzelsystems, sondern noch Variabilität enthält, spricht man auch von einer Referenzarchitektur.

Umsetzung von Vielfalt

Eine weitere Möglichkeit, Variabilität auf architektonischer Ebene zu realisieren, ist beispielsweise, eine Funktion für optional zu erklären (sie kann vorhanden sein oder nicht) oder sogar aus einer Menge gleichartiger Funktionen eine Teilmenge wählbar zu machen. Ein typisches Beispiel wäre eine Menge von Druckertreibern, aus denen bestimmte ausgewählt werden. Ein einfacher Mechanismus, um hier die notwendige Flexibilität auf Architekturebene zu erreichen, wird beispielsweise durch den Publish-Subscribe-Ansatz erreicht. Insgesamt definiert die Architektur der Produktlinie in Kombination mit den explizit definierten Variationsmöglichkeiten die Referenzarchitektur der Produktlinie.

Die Variation zwischen den einzelnen Produkten lässt sich nun in verschiedenster Weise realisieren. Vor allem der Zeitpunkt der Umsetzung der Variation spielt für die Auswahl geeigneter Mechanismen eine zentrale Rolle. Man spricht dabei vom Bindungszeitpunkt. Typische Bindungszeitpunkte sind:

Konfigurationszeit: Beim Auschecken einer Produktvariante eines Konfigurationsmanagementsystems wird Variation bereits insofern berücksichtigt, als dass nur die Komponenten sichtbar werden, die für die Produktvariante relevant sind.

Übersetzungszeit: Beim Übersetzen des Systems wird Variation in das System integriert. Dies kann auch durch Präprozessoren (etwa einen C-Präprozessor) oder aspektorientierte Ansätze (wie AspectJ) geschehen.

Initialisierungszeit: Man bestimmt die konkreten Komponenten, die zu einem System gehören, während des Applikationsstarts (etwa mithilfe von Konfigurationsdateien) und integriert sie dann dynamisch.

Abhängig vom Entwicklungskontext werden meist ein oder zwei Bindungszeitpunkte und die dazugehörigen Mechanismen festgelegt. Beispielsweise könnte man sich in einem Kontext mit Java-Server-Entwicklung dazu entschließen, einerseits wesentliche Anpassungen auf der Ebene des Konfigurationsmanagements abzuhandeln und andererseits feingranulare Variabilitäten auf der Ebene von Konfigurationsdateien und Dynamic Class Loading zu behandeln.

Im Kontext einer performancekritischen C-Entwicklung wiederum ist es sinnvoll, Mechanismen zu nutzen, die keine Auswirkung auf die Laufzeit haben. Hier bietet sich daher beispielsweise die Nutzung des C-Präprozessors an. Dabei ist jedoch wichtig, wie dieses Werkzeug genutzt wird; das heißt, ein systematisches Variantenmanagement muss die Grundlage bilden.

Entscheidend für ein erfolgreiches Variantenmanagement ist, dass Variation durchgehend von der Analyse bis zur Implementierung gemanagt wird. Zudem darf die Nutzung eines Werkzeugs wie des Präprozessors nicht dazu führen, dass über das gesamte System verteilt einzelne Code-Zeilen variabel werden. Dies wiederum erfordert ein Design, das variable Elemente konzentriert und einfach integrierbar macht.

Fazit

Die Entwicklung von Softwareproduktlinien ist ein moderner Ansatz zur effizienten Entwicklung einer Menge miteinander verwandter Softwaresysteme. Der Ansatz beruht nicht nur auf Prinzipien moderner Softwareentwicklung wie der Architekturzentrierung, sondern ist auch offen für verschiedene Software-Implementierungstechniken, etwa Aspektorientierung. Der Ansatz erfordert von einem Unternehmen aber nicht nur technische Kompetenz, sondern auch eine enge Integration der Geschäftsstrategie in die Gesamtentwicklung.

Produktlinienentwicklung wurde weltweit bereits vielfach erfolgreich verwendet, dabei geschah dies in sehr verschiedenartigen Entwicklungsorganisationen. Bei einer erfolgreichen Einführung berichten die Akteure von drastischen Verbesserungen in Bezug auf Entwicklungsdauer und -kosten (Reduktion bis auf ein Zehntel) sowie Qualität (Halbierung der Fehler).

Vor allem die große Flexibilität in der Ausführung des Ansatzes ist einerseits verantwortlich für die Anwendbarkeit, andererseits erfordert sie eine systematische Anpassung an die Unternehmensbedürfnisse. (JS)

PROF. DR. KLAUS SCHMID

beschäftigt sich seit Mitte der 90er-Jahre mit den Themen Requirements Engineering und Softwareproduktlinienentwicklung und kooperiert in diesen Gebieten mit verschiedenen Unternehmen. Er ist Professor für Software Engineering an der Universität Hildesheim.

Literatur

[1] Paul Clements, Linda Northrop; Software Product Lines; Practices and Patterns; Addison-Wesley, 2001

[2] Frank van der Linden, Klaus Schmid, Eelco Rommes; Software Product Lines in Action; Springer, 2007

[3] Product Line Hall of Fame; www.sei.cmu.edu/productlines/plp_hof.html

[4] Klaus Pohl, Günter Böckle, Frank van der Linden; Software Product Line Engineering; Foundations, Principles, and Techniques; Springer, 2007

[5] Frank van der Linden, Klaus Schmid, Eelco Rommes; Software Product Lines in Action; Springer, 2007

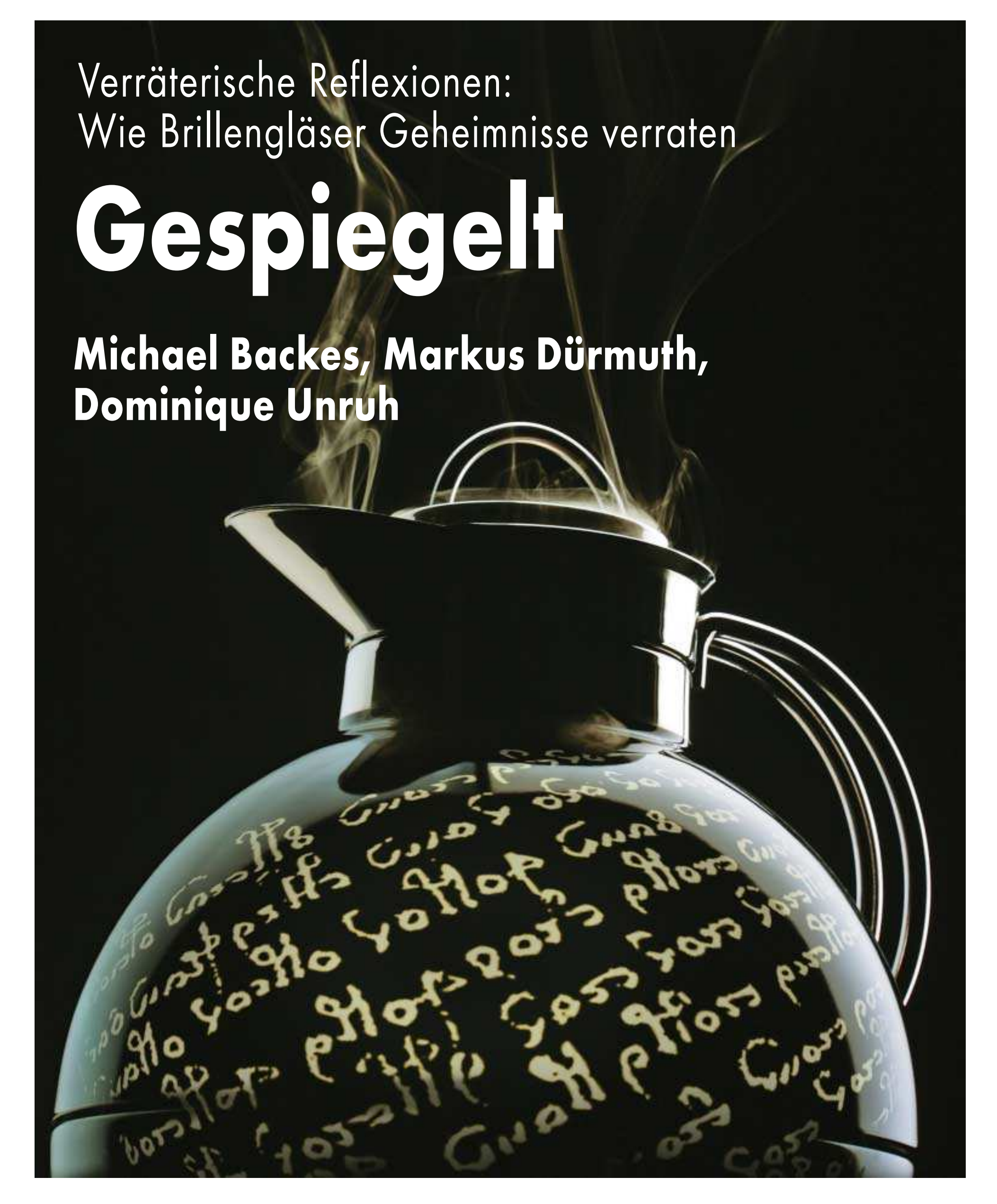
[6] Günter Böckle, Peter Knauber, Klaus Pohl, Klaus Schmid; Software-Produktlinien; Methoden, Einführung und Praxis; dpunkt-Verlag, 2004

Kommerzielle Werkzeuge und -hersteller (Auswahl)

pure::variants (www.pure-systems.com) ist ein Werkzeug zur feature-basierten Konfiguration von Produkten.

Gears (www.biglever.com) setzt hauptsächlich auf dem Konfigurations-management auf.

Metaedit (www.metacase.com) basiert auf der Nutzung von domänen-spezifischen Sprachen.



Verräterische Reflexionen: Wie Brillengläser Geheimnisse verraten

Gespiegelt

Michael Backes, Markus Dürmuth, Dominique Unruh

Alleine in ihrem Büro wähnen Mitarbeiter eines Unternehmens in der Regel ihre Bildschirminhalte vor Ausspähung geschützt – zumal, wenn das Display dem Fenster abgekehrt ist. Doch Reflexionen in Einrichtungsgegenständen können der Spionage Vorschub leisten und vertrauliche Daten Unbefugten zugänglich machen.

Man stelle sich folgendes Szenario vor: Ein Mitarbeiter der Firma XY arbeitet noch spätabends an der Präsentation wichtiger Geschäftszahlen, die am nächsten Morgen fertig sein müssen. Alle anderen Büros sind dunkel, er wähnt sich allein. Doch er ist nicht der einzige, der noch aktiv ist. Im Haus gegenüber, in einem leer stehenden Büro und im Schutz der Dunkelheit nicht zu sehen, steht eine Gestalt neben einem Teleskop.

Da der Mitarbeiter häufig mit sensiblen Daten arbeitet, hat er seinen Monitor so aufgestellt, dass er von draußen nicht zu lesen ist, obwohl er im fünften Stock sitzt. Die Tür ist aus Milchglas und somit undurchsichtig. Er fühlt sich unbeobachtet.

Gefahr auch ohne direkte Sicht

Was er nicht weiß: Der Mann im Büro gegenüber benötigt keine direkte Sicht auf den Monitor, um die Präsentation zu lesen. Er hält Ausschau nach Reflexionen des Monitors in Gegenständen wie Teekannen, Tassen oder Flaschen. Auch im vorliegenden Fall wird er fündig: Der Monitor spiegelt sich in der Teekanne. Noch schlimmer allerdings wäre es gewesen, wenn der Mitarbeiter Brillenträger wäre – darin spiegelt sich der Monitor noch besser.

Es mag auf den ersten Blick kaum überraschen, dass sich Dinge in gläsernen Oberflächen spiegeln. Allerdings war man sich der daraus resultierenden Probleme im Umgang mit sensiblen Daten bisher nicht ausreichend bewusst. Ein Grund dafür könnte die geringe Größe der Reflexion sein: Ein normaler Monitor wird mit einer Größe von etwa 1 cm in der Kanne gespiegelt. Mit einer normalen Kamera und auch mit einem guten Teleobjektiv ist selbst aus relativ kleinen Entfernungen kaum etwas zu erkennen. Die benötigten extremen Vergrößerungen sind nur mit etwas mehr Einsatz lesbar.

Es erfordert dafür schon ein größeres Teleskop und eine gute Portion Fingerspitzengefühl. Komplementiert wird dies durch eine Spiegelreflexkamera und etwas Zubehör. Aus 10 Metern Entfernung kann man mit dieser recht günstigen Ausstattung (Teleskop für circa 300 Euro, Spiegelreflexkamera für circa 600 Euro) bereits kleine Schriften lesen (Abb. 1). Mit teurerem Equipment lassen sich ungleich bessere Resultate erreichen.

Dies mag zunächst nach Science-Fiction klingen, jedoch sind verwandte Szenarien sogenannter kompromittierender Abstrahlung bereits seit Längerem untersucht. Militärische Einrichtungen sollen sich schon seit den 60er-Jahren mit elektromagnetischer Abstrahlung beschäftigen. Die ersten öffentlich bekannten Resultate zu diesem Thema veröffentlichte Wim van Eck 1985. Er zeigte, dass man aus der elektromagnetischen Abstrahlung von Röhrenmonito-

ren und Fernsehern das dargestellte Bild rekonstruieren kann [1]. Doch ist dies nicht das einzige Signal, das sich auffangen lässt. Zahlreiche weitere Quellen haben Forscher seither untersucht, beispielsweise durch Monitorkabel oder serielle Kabel.

Die schlechte Nachricht dabei ist, dass das Verschlüsseln der Daten diese Art von Angriffen nicht abwehren kann, da auf dem Bildschirm angezeigte Daten vom Menschen gelesen werden sollen. Die gute Nachricht ist hingegen, dass sich elektromagnetische Abstrahlung gut abschirmen lässt, ohne den Benutzer übermäßig stark einzuschränken. Das lässt sich durch einen Faradayschen Käfig erreichen, also durch Ummanteln der betroffenen Räume beziehungsweise der betroffenen Geräte und Kabel durch Metallplatten, Folien und Netze. Das Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de) hat Mittel und Modelle entwickelt, um diesen Angriffen zu begegnen.

Andere Monitore, andere Gefahren

Eine andere Form der optischen Abstrahlung untersuchte Markus Kuhn 2002 in Cambridge. Da das Bild eines Röhrenmonitors zeilenweise aufgebaut wird und der Leuchtstoff nur eine kurze Leuchtdauer besitzt (das ist auch der Grund für das Flackern von Röhrenmonitoren bei niedriger Bildwiederholfrequenz), lässt sich das Monitorbild aus dem Flackern des Raumes zurückrechnen [2]. Für LCD-Monitore oder andere Nicht-Röhrenmonitore sind diese Ansätze jedoch nicht anwendbar. Da heutzutage in den meisten Büros LCD-Monitore oder Laptops zum Einsatz kommen, hat diese Bedrohung an Relevanz verloren.

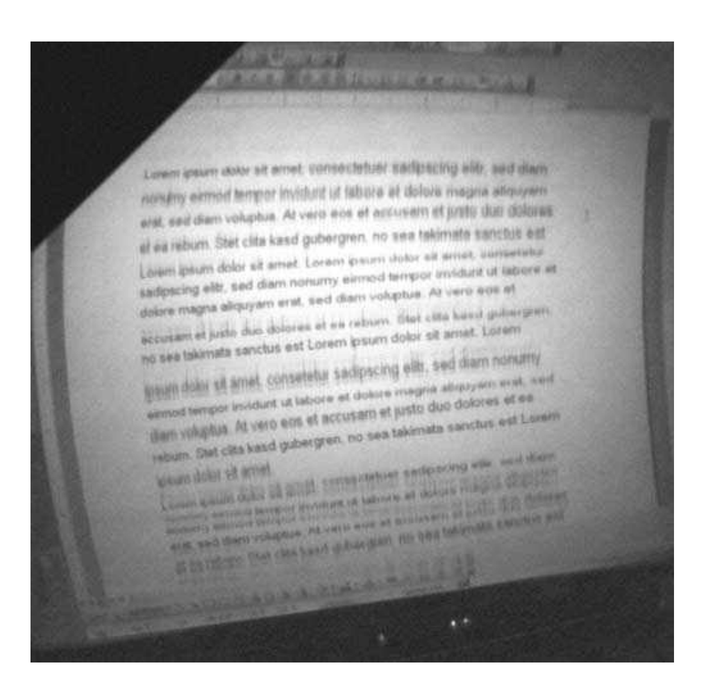
Es stellt sich aber nun die Frage, ob auch LCD-Monitore ausgespäht werden können. Die Arbeit der Autoren [3] zeigt, dass es möglich ist. Dies ist insbesondere deswegen problematisch, weil sich optische Abstrahlung im Gegensatz zu elektromagnetischer kaum abschirmen lässt, ohne den Benutzer zu beeinträchtigen.

Ein Blick in verschiedene Büros zeigt, dass sich auf den meisten Schreibtischen eine Vielzahl von reflektierenden Gegenständen befindet. Dazu gehören beispielsweise Teekannen, Gläser, Tassen und Löffel. Doch es kommt noch schlimmer: Selbst in den Augen des Benutzers sowie in dessen Brillengläsern reflektiert sich der Monitor. Dabei spielt es keine Rolle, ob die Brille entspiegelt ist oder nicht – in beiden Fällen sind gute Reflexionen erkennbar.

Die Qualität der Reflexionen wird im Wesentlichen durch die Krümmung des spiegelnden Gegenstandes und die Beschaffenheit seiner Oberfläche bestimmt. Bei den meisten Teekannen sind die Reflexionen hervorragend, da diese sowohl einen großen Durchmesser (ab circa 12 cm) als auch eine sehr glatte und gut reflektierende Oberfläche (Glas oder Keramik) haben. Entsprechend gut sind die Reflexionen. Ebenso bietet eine Vielzahl anderer Gegenstände vergleichbare Reflexionen, etwa – abhängig von ihrer genauen Form – Tassen und Gläser (sie haben ebenfalls eine sehr gut reflektierende Oberfläche, aber einen etwas geringeren Durchmesser) oder Löffel, wobei hier bisweilen die Oberfläche zu zerkratzt ist.

Gefahr durch Benutzerauge

Während man versuchen kann, die genannten Gegenstände vom Schreibtisch oder besser aus dem gesamten Büro zu entfernen, ist dies für Brillen und Augen nicht möglich. Insbesondere eine Brille bietet durch die geringe Krümmung und die glatte Oberfläche große und wenig verzerrte Bilder (Abb. 2). Entspiegelte Brillen



Schon mit einer Ausrüstung für rund 900 Euro kann man kleine Schriften auf eine größere Entfernung ohne Schwierigkeiten entziffern (Abb. 1).

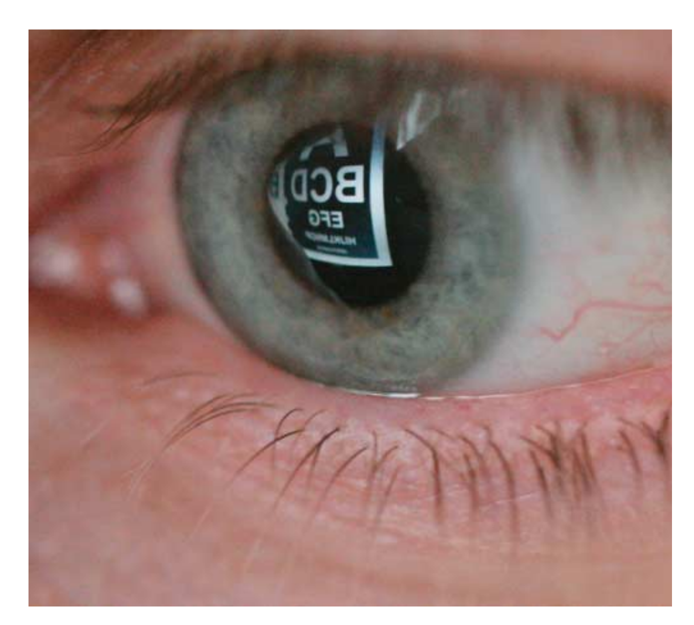


Besonders glatte Oberflächen mit geringer Krümmung ermöglichen hervorragende Reflexionen – auf Brillen, wie hier zu sehen, sogar, wenn diese entspiegelt sind (Abb. 2).

beeinträchtigen die Qualität der Bilder nicht wesentlich: Die abgebildete Brille war entspiegelt. Deutlich anspruchsvoller, aber wissenschaftlich betrachtet auch spannender, sind die Reflexionen im Auge des Benutzers.

Die gute Nachricht ist, dass die Reflexionen im Auge aufgrund seines geringen effektiven Durchmessers (circa 16 mm) sehr lichtschwach sind. Man benötigt daher lange Belichtungszeiten. Gleichzeitig ist das Auge jedoch ständig in Bewegung, wodurch selbst bei Belichtungszeiten von weniger als einer Zehntel-Sekunde massive Verwischungen entstehen. Nichtsdestotrotz zeigt Abbildung 3, die unter idealen Bedingungen aufgenommen wurde, dass das Auge prinzipiell gut reflektiert. Das ist nicht weiter verwunderlich, da es dafür konzipiert ist, die Lichtstrahlen möglichst wenig zu streuen, und daher eine sehr glatte Oberfläche hat.

Auch wenn es gegenwärtig noch nicht möglich erscheint,



Selbst das Auge liefert unter Idealbedingungen wie hier gute Reflexionen – ein Glück, dass diese unter weniger guten Bedingungen durch die schnellen Bewegungen und kurzen Belichtungszeiten stark verwischt sind (Abb. 3).

die Reflexionen im Auge auf größere Entfernungen auszunutzen, so rechnen die Autoren damit, dass in näherer Zukunft durch Verwendung besserer Teleskope und algorithmische Nachbearbeitungen deutliche Verbesserungen erreichbar sind.

Abwehrstrategien entwickeln

Doch selbst bei gut reflektierenden Gegenständen ist nicht alles verloren, denn das Ausspähen von Daten auf diesem Weg funktioniert nachweislich nur dann, wenn bestimmte Bedingungen gegeben sind – die man wiederum dazu verwenden kann, Abwehrstrategien aufzustellen.

Eine Methode zur Abwehr beruht auf dem Prinzip der Diffraktion. Diffraktion ist ein physikalisches Phänomen, bei dem sich Licht, das eine Öffnung passiert, so auffächert, dass aus einem Lichtpunkt eine unscharfe Scheibe wird. Dieses Phänomen ist in der Astronomie bestens bekannt und einer der Gründe dafür, warum man Teleskope mit immer größeren Durchmessern baut.

Für den vorliegenden Fall bedeutet das, dass man die benötigte Größe des Teleskops in einer gegebenen Situation abschätzen kann. Die Tabelle „Minimaler Teleskopdurchmesser“ zeigt einige dieser Werte. Diese lassen sich wie folgt berechnen. Zunächst bestimmt man die Größe des reflektierten Bildes. Dabei fließt die Krümmung der Oberfläche ebenso mit ein wie die Richtung, unter der der Monitor gespiegelt wird. Anschließend bestimmt man den Winkel, unter dem dem entfernten Betrachter zwei Pixel in dem reflektierten Bild erscheinen. Daraus kann mittels des Rayleigh-Kriteriums (benannt nach dem englischen Gelehrten Lord Rayleigh, Physik-Nobelpreisträger 1904) die erforderliche Öffnung des Teleskops berechnet werden.

Minimaler Teleskopdurchmesser

Gegenstand	Distanz	Öffnung
typische Teekanne	5 m	16 cm
	10 m	33 cm
	20 m	66 cm
Auge	2 m	62 cm
	5 m	1,5 m
	10 m	3,1 m

Genauer besagt das Rayleigh-Kriterium, dass zwei Sterne dann noch visuell zu unterscheiden sind, wenn der Winkel (in Grad), unter dem sie dem Betrachter erscheinen, größer ist als das 70-Fache des Quotienten aus der Wellenlänge des Lichts und dem Teleskopdurchmesser. Als Formel:

$$\text{Winkel} > 70 \frac{\text{Wellenlänge}}{\text{Durchmesser}}$$

Das bedeutet auch, dass die Lesbarkeit (beziehungsweise die Entfernung) proportional mit dem Teleskopdurchmesser zunimmt, dass also eine Verdopplung des Durchmessers entweder zu einer Verdopplung des Abstands oder zu einer Halbierung der kleinstmöglichen noch lesbaren Fontgröße führt.

In der Praxis gibt es weitere Faktoren, die diesen Angriff erschweren, sie sind jedoch nicht so leicht abzuschätzen wie der Einfluss der Diffraktion. Zunächst ist dies die benötigte Belichtungszeit. Da mit vergleichsweise extremen Vergrößerungen gearbeitet wird, trifft nur sehr wenig Licht den Sensor der Kamera, die Bilder werden dunkel. Aus 10 Metern Entfernung ist mit Belichtungszeiten zwischen ein und fünf Sekunden zu rechnen. Bei bewegten Gegenständen wie Brillen oder auch bei bewegten Monitorbildern ist das ein Problem.

Ein anderer Faktor ist die Tiefenschärfe. Wie aus der Fotografie bekannt, gibt es genau eine Ebene, die scharf dargestellt wird. Der Vordergrund und der Hintergrund werden, abhängig von der Kamera und dem verwendeten Objektiv, mehr oder weniger unscharf. Während dieser Effekt bei den üblicherweise verwendeten Brennweiten nur moderat auftritt und oft sogar als künstlerisches Mittel gewollt ist, führt er bei den verwendeten Vergrößerungen zu großen Schwierigkeiten. Der Bereich, der noch scharf dargestellt wird, liegt in typischen Situationen im Bereich von Millimetern, geringste Bewegungen des Objekts führen bereits wieder zu Unschärfe.

Abschließend bleibt festzuhalten, dass der beschriebene Angriff erst jüngst bekannt wurde und daher das genaue Ausmaß des Risikos noch nicht endgültig geklärt ist. Man kann gegenwärtig nur dazu raten, Umsicht walten zu lassen. Sollten wichtige Dokumente auf dem Bildschirm angezeigt werden, kann es nicht schaden, die Vorhänge zu schließen. (ur)

PROF. DR. MICHAEL BACKES

hat den Lehrstuhl für Informationssicherheit und Kryptographie an der Universität des Saarlandes inne.

DR. DOMINIQUE UNRUH UND MARKUS DÜRMUTH

sind wissenschaftliche Mitarbeiter am Lehrstuhl für Informationssicherheit und Kryptographie an der Universität des Saarlandes.

Literatur

[1] Wim van Eck; Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? In: Computers & Security; Vol. 4, 1985

[2] Markus G. Kuhn; Optical Time-Domain Eavesdropping Risks of CRT Displays; Proceedings of the 2002 IEEE Symposium on Security and Privacy, May 2002

[3] Michael Backes, Markus Dürmuth, and Dominique Unruh; Compromising Reflections – or – How to Read LCD Monitors Around the Corner; Proceedings of the 2008 IEEE Symposium on Security and Privacy; May 2008



Semantische Ansätze: Kartoo, Sense Engine, Factspotter

Unterwegs zum Finden

Cai Ziegler

Begriffliche Mehrdeutigkeit und mangelndes Textverständnis bei Google und Konsorten lassen die Suche im Web nicht immer zur wahren Freude geraten. Nun sollen semantische Ansätze dies Dilemma ein für alle Mal beseitigen, damit aus der Such- eine Findmaschine entsteht.

Die Aufgabe ist alles andere als trivial und ihre Lösung mutet nahezu wie das Finden des heiligen Grals der Technik an: Es geht um die Realisierung der semantischen Suche. Dieses hehre Ziel schrieb sich schon die in der *iX* viel zitierte Initiative des Semantic Web auf die Flagge, verwarf es jedoch nach kurzer Zeit wieder, denn eine Verwirklichung schien in unerreichbarer Ferne. Was nicht heißen soll, dass das Thema als solches vom Tisch ist. Im Gegenteil.

Noch immer gibt es zahlreiche Bestrebungen, die den derzeitigen Suchansätzen Intelligenz einhauchen wollen. Vor allem in letzter Zeit scheint Bewegung ins Spiel zu kommen, was Ankündigungen wie die Sense Engine von Crystal Semantics oder der Factspotter von Xerox vor Augen führen. Weiterhin wäre hier das groß angelegte und auf politisch höchster Ebene aufgehängte Projekt namens Theseus – jener Nachfolger des gescheiterten deutsch-französischen Quaero-Projekts, das einen Gegenpol zu Google bilden sollte. Theseus ist zwar semantisch, beschränkt sich aber auf einige ausgewählte Anwendungsfelder, wie die Medizin, und soll darum an dieser Stelle außen vor bleiben. Ohnehin gilt es zunächst zu klären, was denn an der semantischen Suche anders ist als an der jetzigen und wie sie sich definitorisch greifen lässt.

Was eigentlich gemeint ist

Wenn Google und andere suchen, läuft das auf rein syntaktischer Basis ab. Der Benutzer gibt eine Folge von Suchbegriffen ein, und die Maschine liefert eine Trefferliste. Wer nach „Police“ sucht, wird Resultate erhalten, die sich sowohl auf die Band als auch auf eine an der Oder gelegene Stadt in Polen beziehen, nebst Informationen über polizeiliche Angelegenheiten im französisch- und englischsprachigen Raum. Die Suchmaschine vermag nicht zwischen syntaktisch äquivalenten Wortformen zu trennen, die über eine gänzlich unterschiedliche Semantik verfügen.

Außer der Handhabung begrifflicher Mehrdeutigkeit (Polysemie) entziehen sich des Weiteren Zusammenhänge zwischen Suchtermen nahezu vollständig der Auffassungsgabe von Suchmaschinen. Wer beispielsweise nach einer Liste mit allen Personen sucht, die vor 10 Jahren eine Bank überfallen haben, dürfte sich schwer tun, diesen Sachverhalt in eine Sequenz von Suchtermen zu gießen. Noch schwieriger wird es beim Durchgehen der Ergebnisliste, die viele Nieten enthalten dürfte: Die Suchmaschinen von heute scannen Dokumente ausschließlich nach dem Auftreten der Suchbegriffe, ohne jedoch den Textzusammenhang wirklich zu verstehen.

Semantische Suche geht genau dies an, jedoch scheiden sich die Geister schon bei deren Definition. Für die einen ist die semantische Suche eine, die die Bedeutung eines Wortes beim Ranking der Dokumente einbezieht und dem Benutzer daraus resultierende Handlungsempfehlungen gibt. Dies könnte dergestalt sein, dass die Suchmaschine beim Eingeben polysemer Begriffe, wie des erwähnten Wortes „Police“, eine Gruppierung der Ergebnisse nach verschiedenen Kategorien vornimmt, wobei jede Gruppe eine der Bedeutungen des Wortes widerspiegelt. Als Urahn dieser Gattung semantischer Suche kann Northern Light gelten; heute jedoch ist diese durch ein Clustering der Resultate schmackhaft gewürzte Websuche nicht mehr online.

Eine weitere geläufige Sichtweise versteht unter semantischer Suche weit mehr als nur die Disambiguierung, das Auflösen der begrifflichen Mehrdeutigkeit. Dort geht es darum, Zusammenhänge und Relationen zwischen den Such-

begriffen formulieren zu können und dadurch der Suchmaschine Fragen zu stellen, wenn möglich in natürlicher Sprache: „In welchen Kinofilmen von Christopher Nolan spielt Christian Bale die Hauptrolle?“ Die Maschine muss hierzu nicht bloß den Inhalt aller in ihrem Suchindex vorhandenen Dokumente verstehen, sondern außerdem die Anfrage des Benutzers richtig analysieren und dessen Ziel deuten können. Keine leichte Aufgabe. Zusätzlich zu diesen beiden Deutungen des Konzepts der semantischen Suche gibt es beliebige weitere, denn die Verwendung des Terminus ist fast so inflationär wie beim allerorten gebrauchten Begriff der Ontologie. Den gängigen Tenor jedoch formulieren die zuvor genannten Auffassungen.

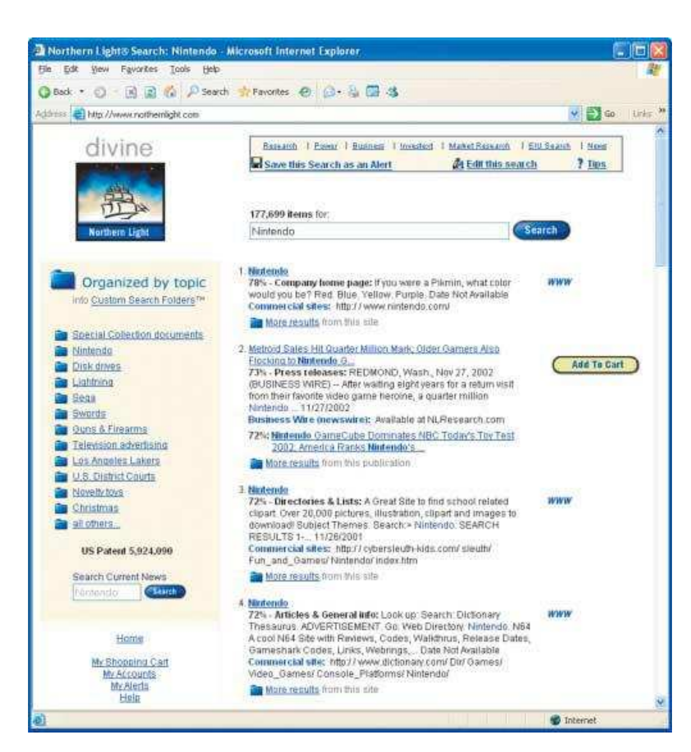
Schubladendenken durchaus erwünscht

Wie eingangs erwähnt, gibt und gab es Suchmaschinen, die der Auflösung von Mehrdeutigkeiten mächtig sind beziehungsweise waren. Die US-Firma Northern Light schaffte mit ihrer gleichnamigen Websuche den ersten Wurf, verschwand aber im Jahr 2002 aufgrund des Verkaufs der Company von der Bildfläche. Was Northern Light von Google und Yahoo unterschied, waren die Ordner, die links neben den typischen Suchmaschinenergebnissen eingeblendet wurden (siehe Abb. 1). Diese gaben sämtliche denkbaren semantischen Kategorien vor, in die sich die Suchergebnisse eingruppieren ließen.

War die Idee durchaus als revolutionär zu bezeichnen, so ließ sich das Gleiche nicht von der Umsetzung behaupten: Die Kategorien schienen oft fragwürdig und nur schwer nachvollziehbar. Dies mag wohl an der Art und Weise der Gruppierung liegen, denn in der Regel ist jene nur wenig semantisch, wie gängige Verfahren lehren.

Um kohärente Gruppen von Texten zu bilden, wird jedes Dokument der Resultatmenge einer Suchanfrage als Vektor dargestellt. Dieser spiegelt die Häufigkeit der Wörter im Text wider. Für jedes Wort wird somit ein Eintrag im Vektor reserviert und dieser mit einer Ganzzahl befüllt. Tritt das Wort „Insight“ beispielsweise dreimal auf, würde an der dazugehörigen Stelle im Vektor eine 3 stehen. Die Abbildung der Dokumente auf Vektoren ermöglicht es schließlich, die Ergebnisse in einem n-dimensionalen Raum als Punkte darzustellen. Mit Clustering-Verfahren (siehe beispielsweise [2]) lassen sich Häufungen von Punkten kenntlich machen, wobei jede Häufung eine Gruppe ausdrückt. Alle diese Gruppen werden bei Northern Light schließlich durch jeweils einen Ordner repräsentiert.

Der Mangel dieses Vorgehens zur Einsortierung der Dokumente in dynamische Gruppen besteht darin, dass das Verfahren wieder nur auf der syntaktischen Ebene arbeitet. Ein Dokument wird in Worte zerlegt, die zum Aufbau des Vektors dienen. Hier kommt es unweigerlich zur Zerstörung von Zusammenhängen, die mehrere Wörter umspannen. Außerdem bleibt die Frage der Synonymie (das Auftreten zweier verschiedener Wörter mit gleicher Bedeutung) sowie der Polysemie außen vor; denn der Vektor zählt nur die Häufigkeit syntaktisch identischer Wortformen. In welchem Kontext ein Wort vorkommt, ob mit Police die Stadt oder die



Northern Lights einstige Websuche gruppierte sämtliche Suchergebnisse ähnlicher Thematik in eigene Cluster (Abb. 1).

Band gemeint ist, findet keine Beachtung.

Verfahren wie Latent Semantic Indexing oder die in der Praxis gängige Singular Value Decomposition (siehe [3]) nehmen sich des Problems an, allerdings schaffen sie ebenfalls keine Abhilfe.

Von Ordnern zu Inseln

Zwar gibt es Northern Lights Suche seit geraumer Zeit nicht mehr im Web, doch haben einige Nachfolger mit ähnlicher Ausrichtung das entstandene Vakuum ausgefüllt. Der spektakulärste unter ihnen dürfte Kartoo sein, eine französische Meta-Suchmaschine, die Resultate der Suche nicht in Ordnern gruppiert, sondern grafisch opulent auf einer Art Landkarte auslegt (siehe Abb. 2). Je größer die räumliche Distanz zwischen den kleinen Inselchen, umso geringer die semantische Ähnlichkeit der beiden Themen-Cluster. Um wieder beim Police-Beispiel zu bleiben, sollten im Idealfall die Dokumente, die sich auf die Band beziehen, und jene, die die polnische Stadt zum Inhalt haben, auf weit voneinander entfernten Archipelen untergebracht sein. Als verwendete Basistechnik darf man bei diesem interessanten Ansatz wohl ein als Self-organizing Maps bekanntes Verfahren annehmen (siehe [4]), bei dem es jedoch mit der Semantik ebenfalls nicht so weit her ist. Darum sind die Ergebnisse von Kartoo oftmals zwar nett anzuschauen, aber durchaus noch verbesserungsfähig.

Um die Zuordnung von Dokumenten zu Themen zu verbessern, hat David Crystal, einer der weltweit führenden Sprachwissenschaftler und Herausgeber der Cambridge Encyclopedia of the English Language, einen neuen Ansatz in Angriff genommen. Das Neue daran ist nicht einmal die Technik, sondern der enorme Aufwand, der betrieben wurde, um das Projektvorhaben zu

iX-TRACT

- Semantische Suche zielt darauf ab, die Bedeutung von Begriffen statt deren lexikalische Formen zu betrachten und in die Suche einzubeziehen.
- Typische Ausprägungen semantischer Suche sind die Disambiguierung mehrdeutiger Anfragen und die Zuordnung von Dokumenten zu Kategorien, die deren Inhalt beschreiben.
- Weitergehende Ansätze semantischer Suche betrachten nicht nur Begriffe und deren Kontext, sondern versuchen außerdem, die grammatikalischen Strukturen von Sätzen und deren Bedeutung zu erfassen.



Die Meta-Suchmaschine Kartoo gruppiert Resultate nicht nur in Ordner, sondern platziert sie wahlweise auf räumlich getrennten Inseln einer Karte (Abb. 2).

realisieren: Über 15 Jahre haben Crystal und seine Mitarbeiter jedes Wort der englischen Sprache genauestens unter die Lupe genommen und klassifiziert. Das nun fertige Produkt wird unter dem Namen Sense Engine vermarktet und gilt als das Flaggschiff des Unternehmens Crystal Reference, das der Linguist ins Leben gerufen hat.

Tatsächlich ist die Sense Engine schon im Einsatz und erwirtschaftet Profit, um die horrenden Entwicklungskosten wieder einzufahren. Allerdings nicht, wie man vermuten mag, in einer Suchmaschine, sondern als Teil einer Softwarelösung für Onlinewerbung: 2006 hat Ad Pepper Crystal Reference geschluckt, ein führendes Unternehmen für Contextual Targeting, der bedarfsgerechten und auf die Interessen des Site-Besuchers zugeschnittenen Platzierung von Werbung. Zuvor hatte Crystal versucht, seine Entwicklung den beiden Giganten Google und Yahoo schmackhaft zu machen, die jedoch dankend ablehnten. Als Grund für die Ablehnung äußerte Crystal in einem Interview in der Online-Ausgabe der FAZ vom 24. September 2007 die Vermutung, dass die beiden wohl schon zu viel Geld in eigene Ansätze investiert hätten, die jedoch nicht richtig gut funktionieren würden und minderwertig seien. Ob hier der verletzte Stolz oder begründete Kritik Vater der Äußerung war, sei dahingestellt.

Was zunächst wie eine 180°-Wende anmuten mag, ist faktisch gar kein so großer Bruch. Denn sowohl beim Contextual Targeting wie bei der Websuche ist der zentrale Punkt die Erkennung des Themas einer Webseite: Bei der Suche ist dies nötig, um Themen-Cluster herauszufinden. Beim Contextual Targeting dient die Kategorisierung hingegen dem Matching der vom Benutzer aktuell betrachteten Seite zu einer Werbebotschaft aus einem Pool von Bannern. Derzeit im Einsatz befindliche Ansätze scheitern oftmals kläglich, wie das Ad-Targeting bei Googles Ad Words oder Youtube beweist. Der Grund hierfür liegt darin, dass das Matching vom Seiteninhalt zur Botschaft rein auf Basis von Schlüsselwörtern, nicht jedoch auf der Basis des semantischen Inhalts durchgeführt wird. Als Negativbeispiel führt Crystal einen hypothetischen Fall an, bei dem zu einem elektronischen Nachrichtenartikel über eine Messerstecherei die Werbung eines Herstellers von Küchenutensilien eingeblendet wird. Das in beiden Fällen vorkommende Stichwort „Messer“ liefert dazu den Anstoß, obwohl der Kontext ein völlig anderer ist.

Wort für Wort fein seziert

Menschlicher Fleiß heißt das Geheimrezept von Crystals Sense Engine, denn im Laufe der zuvor genannten 15 Jahre haben er und seine Helfer ein Klassifikationsschema aus über 2000 Kategorien in Handarbeit erstellt. Das Schema zu konzipieren war dabei jedoch nur der Gipfel des Eisbergs, denn zusätzlich ging sein Team Wörterbücher durch und klassifizierte jeden einzelnen Eintrag gemäß dem Schema. Aufgrund der vielfach zitierten Mehrdeutigkeit von Begriffen können einem solchen Eintrag durchaus viele Bedeutungen zugeordnet sein. So ist „Depression“ nicht nur eine Krankheit, sondern ebenso eine Wetterlage oder ein Terminus aus der Wirtschaft.

Im Fall Police würde dies allein jedoch nicht weiterhelfen, denn in der Bedeutung der Stadt aus Polen wird man Police in keinem Wörterbuch finden: Eigennamen, Namen von Marken, Produkten und weitere sogenannte „Named Entities“ sind Mangelware in Wörterbüchern. Deren Umfang würde sonst schier explodieren, zudem wäre die Aufnahme von Named Entities dem Zweck eines Wörterbuchs nur wenig zuträglich. Crystal hat sich dieser Eigennamen jedoch ebenfalls angenommen und so die Datenbasis der Sense Engine für diverse Domänen um die darin gängigen Entitäten erweitert. Eine Sisyphosarbeit.

Allerdings liegt der Erfolg auf der Hand. Denn dank der Möglichkeit, für jedes textuelle Atom eines elektronischen Dokuments seine optionalen

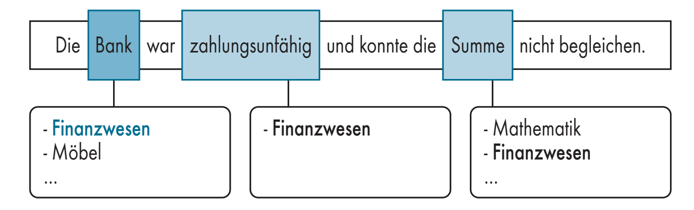
Semantisches Lexikon WordNet

WordNet ist ein groß angelegtes Projekt der Universität Princeton, das darauf abzielt, die Wörter und Begriffe der englischen Sprache semantisch zu strukturieren und deren Bezüge untereinander aufzuzeigen. Der Nukleus von WordNet ist das sogenannte Synset, das für ein abstraktes Konzept steht und sämtliche Wörter umfasst, die synonym für dieses Konzept stehen. Ein derartiges Synset für den Begriff des Flugzeugs würde die Wörter „plane“ und „aircraft“ beinhalten. Neben Synonymen sind oft Beispielsätze für den Gebrauch des Konzepts genannt (Glosses).

Interessanter ist jedoch der Bezug zu anderen Synsets des WordNet, etwa durch Hyponymie zum Ausdruck gebracht: Konzept A gilt als Hyponym von B, wenn A eine Spezialisierung von B darstellt und folglich jede Ausprägung von A automatisch eine Instanz von B ist. So ist „Düsenflugzeug“ ein Hyponym von „Flugzeug“. Es gibt zahlreiche weitere semantische Bezüge, beispielsweise die Meronymie, die eine Teil-Ganzes-Relation ausdrückt, wie „Reifen“ beim Konzept „Fahrzeug“.

WordNets Datenbank gruppiert über 150 000 Wörter in weit mehr als 115 000 Synsets und kann gebührenfrei in verschiedenen Formaten heruntergeladen werden. Zahlreiche verfügbare APIs in verschiedenen Programmiersprachen erleichtern dem Entwickler den Zugriff. Primärer Verwendungszweck von WordNet ist das Umfeld der automatischen Textverwertung, darunter Text Mining, Information Retrieval und Natural Language Processing (NLP). Außerdem ist seine strukturelle Ähnlichkeit zu den vor allem im Semantic Web gebräuchlichen Ontologien deutlich erkennbar.

Außer der englischen Mutterversion gibt es Bestrebungen, das WordNet in 40 weitere Sprachen zu übertragen, unter diesen Deutsch. Allerdings ist das teutonische Pendant namens Germanet nicht frei verfügbar.



Der in der Abbildung gesuchte Sinn des Wortes „Bank" kann dank des umgebenden Kontextes ermittelt werden (Abb. 3).

Kategorien zu bestimmen, lässt sich leicht der im Kontext gebrauchte Sinn eines Wortes herausfinden. Man nehme den Begriff „Chair", der ein Möbelstück (Stuhl) oder eine Person (universitärer Lehrkörper) bezeichnen kann. Treten im kapselnden und in den umliegenden Sätzen weitere Konzepte auf, die dem universitären Umfeld zuzurechnen sind, bei denen deshalb eine Assoziation mit der Kategorie „Universität" vorliegt, ist dies ein stichhaltiges Indiz, dass der Lehrkörper und nicht der Stuhl gemeint ist. Es wird daher die Überlappung der Kategorien für jeden der umliegenden Begriffe in einem nicht zu großen Umkreis gemessen. Die Kategorie mit den meisten Treffern gewinnt (siehe Abb. 3).

Das gezeigte Verfahren ist einfach und keineswegs neuartig, setzt jedoch einen enormen Zeitaufwand voraus. Darum wurde es bislang nur für die englische und nicht für die deutsche Sprache umgesetzt. Zwar gibt es schon gute elektronische Wörterbücher, bei denen die diversen Bedeutungen eines Eintrags vermerkt sind, jedoch sind hier eben meist nur Konzepte und weniger Named Entities angeführt. Zudem liegt kein detailliertes, enzyklopädisches Klassifikationsschema vor, das jeder möglichen Bedeutung die zugehörige Kategorie zuordnet. Typisches Beispiel für ein strukturiertes, digitales Wörterbuch ist WordNet (siehe den Kasten „Semantisches Lexikon WordNet"), das in mehreren Sprachen, hauptsächlich aber in englischer, vorliegt.

Es gibt auch maschinelle Ansätze, bei denen der Rechner lernt, vollkommen automatisch und ohne derartig aufwendiges Zutun des Menschen den richtigen Sinn zu ermitteln. Allerdings funktionieren diese in der Praxis bei Weitem nicht so gut. Crystal hat hier einen Präzedenzfall geschaffen und kann mit einer hohen Güte der Kategorisierung von Dokumenten gemäß dem Klassifikationsschema glänzen, was die von ihm vorgelegten Benchmarks bestätigen.

Aufbruch zu neuen Such-Ufern

Während sich Crystals Sense Engine vornehmlich dem Thema der Disambiguierung von Konzepten verschreibt, geht Factspotter von Xerox einen Schritt weiter. Hier will man laut einiger Pressemeldungen Google und Yahoo Paroli bieten. Mit einer semantischen Suchmaschine, die Anfragen in natürlicher Sprache erlaubt und nicht nur Aneinanderreihungen bloßer Schlüsselwörter.

Mehr noch: Factspotter kann einzelne Passagen als passende Hits für eine Anfrage ausmachen; das kleinste Granulat ist daher nicht mehr ein ganzes Dokument, in dem die Antwort auf die Frage liegt, sondern tatsächlich nur der relevante Absatz. Synonyme erkennt die Suchmaschine aus Grenoble ebenso ohne Schwierigkeiten: Wer in seiner Anfrage an Factspotter nach Larry Ellison sucht, wird sogar Dokumente als Treffer erhalten, die nur vom Vorstandsvorsitzenden von Oracle sprechen, ihn jedoch nicht namentlich erwähnen.

Weiterhin analysiert Factspotter Sätze auf deren grammatikalische Struktur hin. Eine gewöhnliche Suchmaschine weiß mit dem schlichten Personalpronomen „er" nicht viel anzufangen. Da dieses Wörtchen syntaktisch von Larry Ellison verschieden ist, vermag sie nicht den Bezug zum Oracle-Chef zu erkennen. Factspotter erkennt dank einer linguistischen Engine, dass sich das „er" als Subjekt des aktuellen Satzes auf Larry Ellison bezieht, der im vorigen Satz genannt wurde. Beide Sätze wären somit Hits für eine Anfrage nach Ellison.

Welche ausgeklügelten Techniken bei Factspotter unter der Haube bemüht werden, liegt weitgehend im Dunkeln. Ohnehin findet sich im Web herzlich wenig Material zu dieser Suchmaschine der nächsten Generation. Darum lassen sich auch keine stichhaltigen Argumente anführen, die schwarz auf weiß belegen könnten, dass diese tatsächlich hält, was sie verspricht. Zudem lässt Xerox auf seiner Homepage verlauten, dass seine neue Suchmaschinentechnik, entgegen der Aussagen mehrerer Pressemitteilungen, nur für interne Zwecke genutzt würde und somit eben nicht als Gegengewicht zu Google und Yahoo gedacht sei. Jedenfalls noch nicht.

Und wo bleibt das Semantic Web?

Neben allen gezeigten Ansätzen blieb bislang das Semantic Web, das in seinen frühen Manifesten die semantische Suche zum Ziel Nummer 1 erkoren hat, außen vor. Zu Recht, denn noch ist wenig von der Realisierung jener Vision zu verspüren. Dazu müssten erst weite Teile des aktuellen Web semantisch von Menschenhand annotiert werden (siehe [1]), was in weiter Ferne liegt. Sollte dieses Werk eines Tages jedoch tatsächlich vollbracht sein, stünde der semantischen Suche auf Basis annotierter RDF-Tripel nichts mehr im Wege. Passende Anfragesprachen gibt es zuhauf, Requests in diesen könnten relativ leicht in natürliche Sprache übertragen werden und umgekehrt.

Dennoch setzen Experten dem entgegen, dass Suchmaschinen, wie sie das Semantic Web in seiner einen Quantensprung verheißenden Vision vorsieht, in puncto Geschwindigkeit den handelsüblichen Search Engines deutlich unterlegen wären. Bis dahin müssen noch kleinere Brötchen gebacken werden, mit sprachstatistischen Mitteln zur Disambiguierung von Wortbedeutungen, wie bei Northern Light und Kartoo der Fall, oder mit annotierungswilligen Linguisten, wie bei David Crystal und seiner Mannschaft geschehen. Auf jeden Fall dürfte das Thema in Zukunft noch ordentlich für Zündstoff sorgen. (hb)

DR. CAI ZIEGLER

arbeitet als Consultant bei der Siemens AG, Corporate Technology. Dort beschäftigt er sich mit Themen rund um Suche, Data und Text Mining sowie das Semantic Web.

Literatur

[1] Cai Ziegler; Sinn oder nicht Sinn; Vom Suchen und Finden der Semantik im Web; c't 21/2007, S. 172

[2] Jiawei Han, Micheline Kamber; Data Mining: Concepts and Techniques; Second Edition; San Francisco (Morgan Kaufmann) 2006

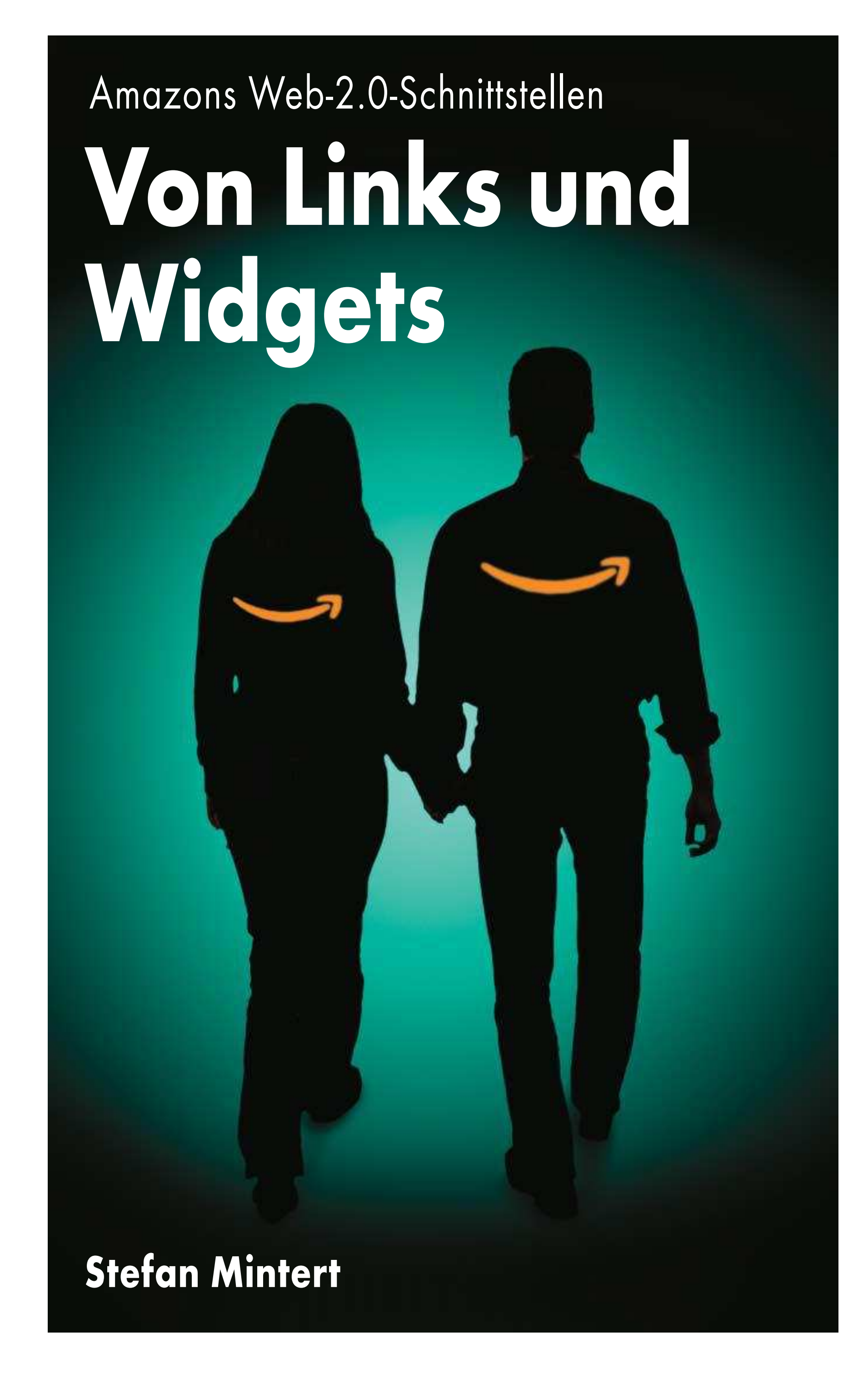
[3] Soumen Chakrabarti; Mining the Web; San Francisco (Morgan Kaufmann) 2003

[4] Cai Ziegler; Kleine Inselmusik; Datenvisualisierung mit Self-organizing Maps; *iX* 02/2008, S. 124



Onlinequellen

Meta-Suchmaschine Kartoo	www.kartoo.com
Semantisches Lexikon WordNet	wordnet.princeton.edu
Whitepapers zur Sense Engine	www.crystalsemantics.com



Amazons Web-2.0-Schnittstellen

Von Links und Widgets

Stefan Mintert

Amazon hat schon vor einigen Jahren eine API bereitgestellt, die es Programmierern erlaubt, Produkte des Internethändlers auf eigenen Webseiten anzubieten. Im Web-2.0-Zeitalter ermöglichen das vereinfachte Schnittstellen und zusammenklickbare Widgets – ohne Programmierkenntnisse.

Das als Internetbuchhändler gestartete Einkaufsportal Amazon hat früh damit begonnen, mit einem Partnerprogramm Dritten zu erlauben, Kunden auf seine Seiten zu locken. Dafür stehen Webservices zur Verfügung (siehe [1]). Es ist jedoch eine einfache Erkenntnis, dass eine Funktion umso häufiger genutzt wird, je simpler sie gestaltet ist.

Links sind Schnittstellen, die Amazon seit Langem anbietet. Die Idee, damit Geld zu verdienen, ist schnell umgesetzt: Ein Interessent registriert sich als Amazon-Partner. Dieser Schritt steht jedermann offen. Die nachfolgenden Geschäfte gelten laut FAQ (siehe Onlinequellen [a]) als „Handelsvermittlung“, „Vermittlung von Geschäften im Internet“ oder Ähnliches. Wer potenziellen Ärger vermeiden möchte, sollte diese Frage mit seinem Steuerberater klären.

Als Ergebnis der Registrierung erhält der frisch gebackene Partner eine ID, die bei allen weiteren Maßnahmen die richtige Zuordnung sicherstellt. Eine solche ID könnte „linkwerkcom-21“ sein. Wer nun einen Link auf ein einzelnes Produkt einrichten möchte, muss nichts weiter tun, als die ID an der richtigen Stelle als Parameter an den Link zu hängen. Der sicherste Weg führt über den Linkgenerator auf der Webseite von Amazon (siehe die Abbildungen 1 und 2). Der dort erzeugte Code nimmt beispielsweise die Gestalt von Listing 1 an. Wer diesen Link oder die unten folgenden, spannenderen Widgets in Aktion sehen möchte, findet sie im Blog des Autors (siehe „Onlinequellen“).

Bei obigem Beispiel handelt es sich um einen Grafiklink. Amazon stellt die dazugehörige Grafik, in diesem Fall den Umschlag des verlinkten Buches, für solche Zwecke zur Verfügung. Ein neues Feature dieser alten Schnittstelle ist der sogenannte Vorschaulink. Er stattet Einzeltitellinks mit einem Mouseover-Effekt aus, bei dem der Betrachter eine Produktvorschau sieht, sobald er die Maus über den Link bewegt. Für die Implementierung von Vorschaulinks genügt es, ein *script*-Element in die eigene Seite einzubauen. Es lädt den diesbezüglichen Widget-Code und erzeugt die Effekte.

Das (gemeinsame) Geldverdienen beginnt, sobald ein Besucher dem Link folgt und bei Amazon einkauft. Der mit der ID „getaggte“ Link stellt sicher, dass Amazon den Vermittler erkennen und für getätigte Einkäufe eine sogenannte Werbekostenerstattung gutschreiben

kann. Die Höhe der Gutschrift liegt derzeit im einstelligen Prozentbereich, bezogen auf den Netto-Umsatz. Neben einem Abrechnungsmodell mit einem festen Prozentsatz gibt es das attraktivere Modell mit gestaffelten Sätzen, je nach Anzahl der verkauften Produkte. Die Konditionen sind auf der Partner-Site zu finden.

Unterwegs von Web 1 zu Web 2

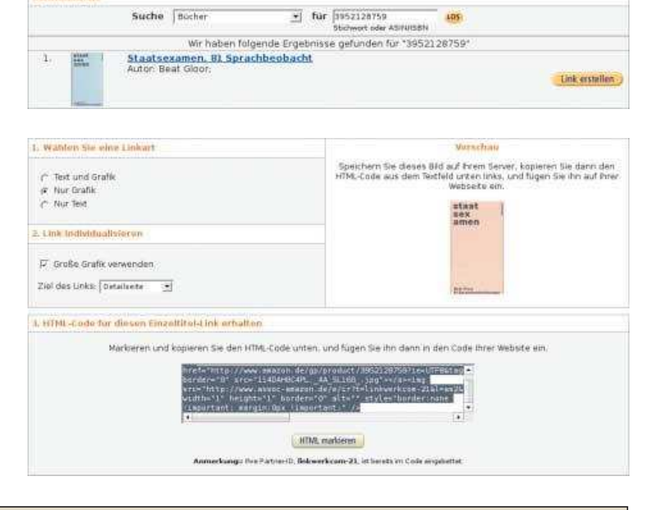
Es ist nicht überraschend, dass es neben dem Einzeltitellink schon früh weitere Optionen gab. Der Klassiker ist sicher das Banner. Amazon stellt nach Produktlinien (Musik, Bücher, Filme, Elektronik et cetera) und nach Größe sortierte Banner zur Verfügung. Mit der Partner-ID versehen, funktionieren sie genauso wie die Einzeltitellinks. Gleiches gilt für „empfohlene Produktlinks“ und „Suchfeld-Boxen“.

Erstere funktionieren über die Vorauswahl einer Produktlinie und eines Schlagworts. Wer etwa „Musik“ und „Country“ vorgibt, erhält den HTML-Code für einen *iframe*, in dem Produkte von Johnny Cash bis Texas Lightning erscheinen.

Suchfeld-Boxen sind klassische HTML-Formulare für die Suche auf Amazon.de, allerdings in einen *iframe* eingebettet. Suchergebnisse werden nicht auf der ursprünglichen Seite des Partners angezeigt, sondern auf der des Internethändlers.

Abgesehen von den Einzeltitellinks arbeiten alle vorgestellten Funktionen mit Code von der Amazon-Seite. Entweder eingebettet in einen *iframe* oder als nachgeladener Scriptcode. Hier zeigt sich, dass obwohl ein Feature noch „Link“ heißt, es sich technisch längst um etwas handelt, wofür sich in den vergangenen Monaten der Begriff „Widget“ etabliert hat. In allen gezeigten Fällen findet ein parametrisierter Zugriff über eine öffentliche API statt. Das Ergebnis ist eine Mashup-Seite. Schon die einfachen Beispiele sind deshalb dem Schlagwort „Web 2.0“ zuzuordnen.

Außer der technischen Umsetzung hat Amazon die Darstellung und die Funktionsvielfalt kontinuierlich erweitert. Eine aufwendigere Funktion sind die „Self-opimizing Links“. Die sich selbst optimierenden Links verändern ihren Inhalt je nach dem der Webseite, in die sie eingebettet sind. Das funktioniert wie bei Googles Werbeeinblendungen. Ein Amazon-Crawler



Erster Schritt zu einem „Einzeltitellink“ ist die Produktsuche. Beim Konfigurieren des Links (zweite Abbildung) bildet der Linkgenerator die gewünschte Darstellung im HTML-Code ab (Abb. 1 und 2).

Listing 1: Von Amazon erzeugter Link

```
<a href="http://www.amazon.de/gp/product/3952128759?ie=UTF8&tag=linkwerkcom-21&linkCode=as2&camp=1638&creative=
    6742&creativeASIN=3952128759"><img border="0" src="114DAHOC4PL._AA_SL160_.jpg">
    </a><img src="http://www.assoc-amazon.de/e/ir?t=linkwerkcom-21&l=as2&o=3&a=3952128759"
    width="1" height="1" border="0" alt="" style="border:none !important;margin:0px !important;" />
```

besucht die Seite, die den selbst optimierenden Link enthält und analysiert deren Content. Die gesammelten Informationen sind die Grundlage für die in Zukunft dargestellten Produkte. Wer die Crawler-Besuche in seinen Zugriffsstatistiken verfolgen möchte, sollte nach der User-Agent-Kennung „Mozilla/5.0 (compatible; AMZNKAssocBot/4.0)“ Ausschau halten. Listing 2 enthält den erforderlichen Code für die selbst optimierenden Links.

Listing 2: Code für selbst-optimierende Links

```
<script type="text/javascript"><!--
  amazon_ad_tag      = "linkwerkcom-21";
  amazon_ad_width    = "468";
  amazon_ad_height   = "60";
  amazon_ad_logo     = "hide";
  amazon_ad_discount = "remove";
//-->
</script>
<script type="text/javascript"
  src="http://www.assoc-amazon.de/s/ads.js"></script>
```

Produkte selbst auswählen

Im ersten Scriptblock sind die über die Webseite ausgewählten Parameterbelegungen zu sehen. Der zweite lädt den Widget-Code. Da die Selbstoptimierung eben nicht von selbst, sondern nur mit dem Crawler funktioniert, versteht es sich, dass der Zugriff auf die Webseite nicht eingeschränkt sein sollte. Im Intranet oder in passwortgeschützten Bereichen öffentlicher Sites steht die Funktion nicht zur Verfügung.

Wer die Kontrolle über die angezeigten Produkte behalten möchte, ist mit dem „Meine Favoriten-Widget“ gut beraten. Über die Webseite lassen sich beliebige Produkte auswählen und zu einem Widget zusammenfassen. Es kann mehrere solcher Zusammenfassungen geben, die der Benutzer jeweils mit einem Namen versehen, speichern und nachträglich ändern kann. Die Verwaltung der eigenen Widgets ist bequem. Im Gegenzug offenbart der erzeugte Code keine Anhaltspunkte für manuelle Parameteränderungen (siehe Listing 3).

Ähnlich sieht das Wunschzettel-Widget aus. Ein Wunschzettel ist eine Funktion, die dazu dient, sich gewünschte Produkte zu merken und für andere sichtbar zu machen. Dazu gehören Verwaltungsfunktionen wie „Wie oft gewünscht?“ et cetera. Aus einer solchen Liste lässt sich direkt ein Widget erzeugen. Es genügt die Angabe einer Mailadresse. Die vorhandenen Wunschzettel zeigt Amazon an und erzeugt auf Klick den Widget-Code. Das Ergebnis ist eine dynamische Webseitenkomponente, die das Blättern in den Produkten und eine Sortierung nach Datum der Aufnahme

iX-TRACT

- Amazon bietet neben einer Webservice-API einfache Schnittstellen für die Verknüpfung der eigenen Webseite mit dem Internet-Händler.
- Für die Benutzung der Widgets genügen minimale Kenntnisse über den Aufbau von Webseiten. Amazon generiert den erforderlichen Code.
- Das Design der Widgets folgt dem Web-2.0-Trend.

und letzter Änderung am Wunschzettel gestattet.

Doch nicht nur im Bereich grafisch aufgepeppter Widgets hat Amazon Neues zu bieten, textuelle Links erfahren ebenfalls eine Modernisierung. Wie oben steht die Einfachheit im Vordergrund. Die Rede ist vom „Quick Link Widget“. Grundlage ist ein kleines Javascript, das über Angabe der Partner-ID einmalig in die Webseite einzubauen ist. Auf den Code sei hier verzichtet, da er neben einem unverständlich parametrisierten URI nichts enthält. Ist der Widget-Code erst auf der Seite aktiv, lassen sich leicht Links einbauen. So nimmt der Verweis auf die Suchfunktion von Amazon nun folgende Gestalt an.

```
<a type="amzn">Walkabouts</a>
```

Hier sollte Musik der Walkabouts als Ergebnis erscheinen, aber Amazon liefert Treffer aus allen Produktlinien. Wer ausschließlich auf Bücher von oder über Bob Dylan, nicht jedoch auf CDs verweisen möchte, fügt die diesbezügliche Kategorie als Attribut hinzu. Und wenn sich Linktext und Suchbegriff unterscheiden sollen, hilft ein weiteres Attribut:

```
<a type="amzn" search="Bob Dylan"
 category="books">Bücher von oder
 über Bob Dylan</a>
```

An diesem Punkt wird klar, dass die Vorgehensweise nichts für HTML-Puristen ist. Das Attribut *type* ist in HTML bekannt, die beiden anderen jedoch nicht. Wer den Code nicht per Hand in eine Seite einbaut, sondern mit irgendeiner Art von Software erzeugen oder verarbeiten lässt, sollte auf eine Validierung verzichten. Bei der Validierung gegen eine HTML/XHTML-Standard-DTD sorgen nicht nur die unbekannten Attribute, sondern auch die in Listing 1 und 3 gezeigten „&“-Zeichen für Fehler. Letztere lassen sich vermeiden, wenn man das „&“ durch „&“ ersetzt.

Quick Link Widgets vereinfachen nicht nur den Suchlink, die Einzeltitellinks lassen sich mit ihrer Hilfe ebenfalls ohne Zusammenklicken auf der Webseite erstellen. Es genügt, die Amazon-eigene Produktnummer namens „ASIN“ zu kennen. Sie ist auf den Produktseiten zu sehen und kann von dort kopiert werden. Ein Link auf ein bestimmtes Produkt sieht so aus:

```
<a asin="B00008Z5G7"
 type="amzn">The Wild, The Innocent &amp;
 The E-Street Shuffle</a>
```

Mit „Meine Favoriten“ kann der Benutzer steuern, welche Produkte das Widget anzeigt (Abb. 3).

Listing 3

```
<script charset="utf-8" type="text/javascript" src="http://ws.amazon.de/widgets/q?ServiceVersion=20070822&MarketPlace=
                         DE&ID=V20070822/DE/linkwerkcom-21/8001/9e647895-aa87-4e83-bc57-87f26a854fe8"> </script>
```

Optische Spielereien

Das Web 2.0 hat Tag Clouds hervorgebracht, die zusammenhängende Darstellung von Begriffen, wobei Schriftgrad und -gewicht dem Stellenwert des jeweiligen Begriffs entsprechen. Der Stellenwert lässt sich auf unterschiedliche Weise berechnen. Wenn es um Tagging geht, dürfte die Häufigkeit eines Tags die maßgebliche Größe für die Berechnung des Stellenwerts sein.

Amazon hat diese visuelle Darstellungsform aufgegriffen und stellt sie als „Product Cloud“ zur Verfügung (siehe Abbildung 4). Die Product Cloud zeigt – wie die selbstoptimierenden Links – Produkte, die dem Inhalt der Webseite nahestehen. Je näher, desto größer und fetter erscheint die Produktbezeichnung. Die Auswahl der Produkte setzt ebenfalls den Besuch des Crawlers voraus.

Ein zweites, visuell aufwendigeres Widget ist die Slideshow, mit Flash realisiert. Der Benutzer wählt – wie bei den Favoriten – über die Webseite beliebige Produkte aus und fasst sie in einer Slideshow zusammen. Es stehen mehrere Größen und Arten von Slideshows zur Verfügung. Einen optional einzugebenden Kommentar legt das Flash-Applet über die Produktabbildung.



Von den Tag Clouds des Web 2.0 inspiriert: die Product Cloud (Abb. 4)



Für die Slideshow stehen mehrere Darstellungsarten und Übergänge zur Verfügung (Abb. 5).

Die Übergänge lassen sich hinsichtlich Art und Geschwindigkeit steuern.

Die guten alten Suchfeld-Boxen hat Amazon im Web-2.0-Stil aufpoliert. Aus ihnen ist nun das Such-Widget geworden. Es handelt sich um eine Webseiten-Komponente, deren Größe und Aussehen wie üblich wählbar sind. In ihr kann ein Benutzer nach Produkten suchen, die im Gegensatz zu den alten Suchformularen innerhalb des Widgets angezeigt werden. Der Benutzer verlässt die Seite erst, wenn er auf ein Produkt klickt.

Context Links von eigenen abgrenzen

Als einfache und wohl mächtigste Verlinkungsmöglichkeit stellt Amazon die sogenannten „Context Links“ zur Verfügung. Für die Benutzung ist lediglich ein *script*-Element in die eigene Webseite einzubauen. Den Rest erledigen der Crawler und das Script. Wie bei einigen Widgets zuvor basiert die Verlinkung auf einer Analyse der Seite. Anstelle von abgesetzten Boxen, die erkennbar als Amazon-Werbung gekennzeichnet sind, erfolgt hier jedoch eine Verlinkung des Textes der Webseite. Geeignete Begriffe werden mit Links auf Amazon-Produkte versehen. Ein Mouseover-Effekt sorgt für eine Vorschau noch vor dem Klick.

Darstellung und maximale Anzahl der Links lassen sich konfigurieren. Bei der Darstellung kann man auf die von Links der jeweiligen Webseite zurückgreifen. Was auf den ersten Blick ganz praktisch aussieht, hat einen entscheidenden Nachteil. Der Leser kann die Amazon-Links nicht von „normalen“ unterscheiden. Damit ein Leser die Seite nicht schnell verlässt, nachdem er ein paarmal frustriert einem Link folgen wollte und immer bei Amazon landete, erscheint es sinnvoller, die Amazon-Links optisch deutlich von eigenen abzusetzen.

Shops per Mausklick

Als Ergebnis erhält man ein Feature, das gelegentlich unerwartete Verknüpfungen herstellt. Der Autor hat es bei einem online veröffentlichten Buch (siehe Kasten „Onlinequellen“) ausprobiert. Dort ist im Abschnitt 2.3 von einem gewissen Stanley Rice die Rede. Amazons Context-Link-Widget verbindet den Namen mit dem Buch „The Years of Rice and Salt“ des Autors Kim Stanley Robinson. Die Wortübereinstimmung ist offensichtlich und dennoch ist der Link nicht das, was man sich wünscht.



aStore: Ein eigener Onlineshop durch nur wenige Mausklicks – mit frei wählbarem Angebot, Einkaufswagen und Produktempfehlungen (Abb. 6)

Die Königsklasse der Widgets ist wohl der „aStore“, ein vollständiger Shop, der als Komponente in jede Webseite einzubetten ist. Anwender können ihn mit beliebigen Produkten aus beliebigen Produktlinien bestücken. Die Farben lassen sich so wählen, dass sich der Shop, der in einem *iframe* läuft, perfekt in die eigene Webseite integriert.

Selbstverständlich erlaubt Amazon mehrere Shops anzulegen, mit Namen zu versehen und nachträglich zu ändern. Außer der festen Partner-ID kann man verschiedene Tracking-IDs benutzen, um in der Abrechnung erkennen zu können, welches Widget beziehungsweise welcher Shop welche Umsätze generiert.



Amazon unterstützt verschiedene Blogging-Plattformen (Abb. 7).

Abschließend sei erwähnt, dass die Widget-Erzeugung auf zahlreiche Blogsites vorbereitet ist, von Wordpress über Blogger bis zu Myspace. Der Benutzer bekommt detaillierte Anleitungen zur Integration des erzeugten Codes in sein Blog.

Fazit

Amazon stellt mit seinen Widgets einfache und sinnvolle Werkzeuge zur Verfügung. Für den Benutzer, der mit seiner Site Geld verdienen möchte, sind die Schnittstellen zu Amazon im Vergleich zu den Anfangszeiten gleichzeitig einfacher und funktionsreicher geworden. Die Unterstützung beliebter Blogsites zeigt eindeutig, dass Amazon die Zielgruppe der Web-2.0-Aktivisten ansprechen will. (hb)

STEFAN MINTERT

ist Geschäftsführer von Linkwerk.com und arbeitet im Bereich XML und Semantic Web 2.0.

Literatur

[1] Macherius, Ingo; Web Services; Handelspartner; Produktdaten von Amazon nutzen; *iX* 6/2004, S. 123

iX-Link0805122

Onlinequellen

[a]	Amazons Partnerprogramm	partnernet.amazon.de/
[b]	FAQ zum Partnerprogramm	partnernet.amazon.de/gp/associates/join/faq.html
[c]	alle Widgets des Artikels online	blog.linkwerk.com/entry/sm/2008-03-01T19.45.00
[d]	Context Links in „XML in der Praxis“	www.linkwerk.com/pub/xmlidp/2000/



Flexibel programmieren mit dem Fluent Interface

Flüssiger Erbauer

Bernd Schiffer

Diverse Paradigmen sollen Entwicklern helfen, große Projekte klar zu strukturieren und den Überblick zu bewahren. Nicht immer geht das einher mit Verständlichkeit und guter Lesbarkeit von Programmen. Das Entwurfsmuster Builder zusammen mit dem Fluent Interface können hier helfen.

Das Entwurfsmuster „Erbauer“ (Builder) ist in die Jahre gekommen. Neue Möglichkeiten beim Erstellen komplexer Objektgeflechte ergeben sich bei der Implementierung einer sogenannten „flüssigen Schnittstelle“ (Fluent Interface, siehe „Onlinequellen“ [a]). Dieser Artikel beschreibt evolutionär in wenigen Schritten eine solche Schnittstelle, ausgehend von einer klassischen Objekterzeugung.

Bei großen Applikationen spielt fast immer die Anbindung externer Systeme eine Rolle. Hierbei werden Daten ausgetauscht, die ein Drittsystem meist in einem vorgegebenen Format übermitteln soll. In vielen Fällen handelt es sich dabei nicht um Standards wie XML, sondern um proprietäre Formate. Eins davon soll diesem Artikel als Beispiel dienen. Das Format besteht aus Abschnitten, von denen jeder eine Menge von Werten aufnimmt, die an bestimmten Stellen des Abschnitts notiert werden. Eine formale Spezifikation dieses Formats sieht so aus:

```
(Abschnitt($stelle:wert)*$)+
```

Zu lesen ist diese Notation wie folgt: „Mindestens ein Abschnitt nimmt beliebig viele Tupel von Stellen zu Werten auf, wobei vor jedem Tupel ein Dollarzeichen steht und jedem Abschnitt ein Dollarzeichen folgt.“ Ein Beispiel wäre:

```
abschnitt$1:wert$3:anderer_wert$anderer_ ↵
                    abschnitt$42:wieder_anderer_wert
```

Dieses Beispiel soll als Anschauungsobjekt für eine API dienen. Deren Code ist in einer für viele deutschsprachige Projekte typischen Mischform aus deutscher und englischer Sprache gehalten. Der Vorteil dabei ist, dass beim – zumindest national gesehen deutschsprachigen – Kunden Begriffe wie Abschnitt, Wert und Stelle zum Sprachgebrauch gehören und die Entwickler somit weniger Kontextwechsel durchführen müssen, als wenn sie diese Begriffe ins Englische übersetzten.

Feste API unterbindet Flexibilität

Eine klassische API für diesen Anwendungsfall besteht aus den zwei Klassen *Abschnitt* und *AbschnittUtil*. Listing 1 zeigt einen Ausschnitt der Testklasse *AbschnittTest*. Abschnitte können demnach Werte für Stellen aufnehmen, und man kann diese Werte für eine bestimmte Stelle wiederfinden. Um den Abschnitt zu erzeugen, erfolgt zunächst seine Instanziierung über einen Default-Konstruktor. Per Setter für die Instanzvariable *name* wird der Abschnittsname gesetzt. Schließlich werden zwei Werte an zwei verschiedene Stellen geschrieben.

Der Test benötigt eigentlich „einen *Abschnitt* mit Namen *abschnittsname* mit Wert *a* an Stelle *1* und mit Wert *b* an Stelle *2*“. Tatsächlich aber wurde ihm bislang etwas vorgesetzt, was zusammengefasst und ohne Variablen so aussieht:

```
Abschnitt abschnitt = new Abschnitt();
abschnitt.setName("abschnittsname");
abschnitt.add(1, "a");
abschnitt.add(2, "b");
```

Dies liest sich weitaus holpriger als im normalen Sprachgebrauch. Es ist faszinierend, zwei Programmierern dabei zuzuhören, wie sie sich gegenseitig beispielsweise beim Pair Programming Code dieser Art vorlesen. Anstatt so etwas zu sagen wie „Hier benötigen wir einen Abschnitt mit Namen *abschnittsname* mit Wert *a* an Stelle *1*“, was ein grammatikalisch korrekter deutscher Satz wäre, sagen sie etwa „Hier machen wir einen *new Abschnitt* und setzen danach den *abschnittsname*n und dann *adden* wir noch *1* Komma *a*“.

Ein naiver Ansatz zur Lösung dieses Lesbarkeitsproblems ist die Ein-

führung eines entsprechenden Konstruktors, etwa:

```
public Abschnitt(String name,
                Abschnittseintrag eintrag...){
  /* Implementierung */}
```

Hierbei ist ein *Abschnittseintrag* nur eine Hilfsklasse zur Aufnahme einer Stelle und eines dazugehörigen Wertes. Der Aufruf erfolgt dann so:

```
Abschnitt abschnitt =
   new Abschnitt("abschnittsname",
   new Abschnittseintrag(1, "a"),
   new Abschnittseintrag(2, "b"))
```

Damit ist die Konstruktion eines Abschnitts auf eine Anweisung reduziert, allerdings auf Kosten der Flexibiliät: Für jede anderweitige Konstruktion eines Abschnitts müsste der Konstruktor respektive die *Factory*-Methode überladen werden, etwa wenn Abschnitte mit IDs, Validatoren, Konvertern, Typen und anderen für die Konstruktion nötigen Teilen gebaut würden. Da wäre die Übersicht bald nicht mehr gegeben, und ein armer Programmierer mag sich bald fragen, welchen der vielen Konstruktoren er aufrufen muss. Nicht gut.

Erforderlich ist zudem, dass der Programmierer weiß, ob das gerade gebaute Objekt konsistent ist. Eine kurze Definition für die Konsistenz eines Abschnitts besagt: „Ein Abschnitt muss immer einen Namen haben. Er darf keine bis beliebig viele Stelle-Wert-Paare haben.“ Diese Information steht jedoch nicht zum Konstruktionszeitpunkt – also beim Programmieren – zur Verfügung, sondern zeigt sich gegebenenfalls erst zur Laufzeit durch schwer nachvollziehbare Fehlermeldungen. Das heißt, Entwickler haben es mit einer unlesbaren, unflexiblen, unübersichtlichen und inkonsistenten – einer fest(gefahren)en – API zu tun.

Zartschmelzende API gefährdet Konsistenz

Stattdessen lässt sich ein Abschnitt auch folgendermaßen konstruieren:

```
Abschnitt abschnitt =
     Abschnitt.mitNamen("abschnittsname")
     .mitWert("a").anStelle(1)
     .undMitWert("b").anStelle(2);
```

Diese Konstruktion liest sich wie die umgangssprachlich Formulierung oben, lediglich ein paar sprachbedingte Punktionen stören noch die freie Rede. Diese Art der Erzeugung gegen eine Schnittstelle, die solch eine flüssige Formulierung zulässt, nennt sich Fluent Interface. Es ermöglicht dem Entwickler den Sprung von einer API hin zu einer DSL, einer Domain Specific Language [b, c], die die Konstruktion von Objekten für den Anwender einer Schnittstelle stark vereinfacht. Martin Fowler und Eric Evans haben diesen Begriff geprägt und das Pattern herausgearbeitet. Die flüssigen Schnittstellen sind stark im Domain Driven Design [1] vertreten, ihre Wurzeln reichen jedoch deutlich weiter zurück: Smalltalker und Lispler sind in der Regel damit vertraut. Es gibt aber auch in modernen Programmiersprachen mittlerweile gute Beispiele für die Anwendung dieses Pattern, etwa Java-Bibliotheken wie JUnit, Easymock und JMock oder die Web-Frameworks Ruby on Rails und Grails.

Die Implementierung einer flüssigen Schnittstelle ist ungleich anspruchsvoller als die einer klassischen, festen. Ein naiver Ansatz, der – euphemistisch gesehen – eher zartschmelzend als flüssig daherkommt, sähe aus wie Listing 2.

Damit kann ein Benutzer einen Abschnitt schon flüssig konstruieren. Es fällt zunächst auf, dass Setter-Methoden einen Rückgabewert haben können, hier jeweils das zu konstruierende Objekt. Erst diese Eigenschaft der Setter einer flüssigen API ermöglichen eine Aneinanderreihung von Methodenaufrufen und damit einen grammatikalisch korrekten Satzbau.

Hinzu kommt, dass diese Notation von der in Java verbreiteten Konvention abweicht, für Methoden Befehle in Form von Imperativen zu verwenden, etwa *initialisiere()*, *add()* oder *getFoo()*. Der Vorteil der Konvention ist, dass beim Blick auf die an einem Objekt aufzurufenden Methoden anhand des Methodennamens klar wird, welche Befehle das Objekt entgegennehmen kann.

Bei einem flüssigen Interface gibt es viele Methoden, deren Namen wenig Aussagekraft über ihre Verwendbarkeit haben. Beispiele dafür sind *mit*, *in*, *undMit* oder *anStelle*. Diese Methoden sind nur aus dem Kontext, also dem Satzbau, heraus interpretierbar. Es ist zwar recht einfach, flüssige Schnittstellen als solche aufgrund der Methodennamen zu identifizieren und sich als Programmierer von der vorgegebenen Grammatik leiten zu lassen, jedoch steigt der Schwierigkeitsgrad mit der Größe der Schnittstelle.

Lesbarer ist die Objektkonstruktion mittlerweile und flexibler ebenfalls: Die Methoden lassen sich beliebig miteinander verknüpfen. Neue Attribute am Objekt kann man quasi sofort bei der Konstruktion verwenden und muss sie nicht erst in die Konstruktoren einarbeiten. Allerdings schießt diese Flexibilität weit übers Ziel hinaus, denn wenn die Me-

Listing 1: Ausschnitt aus *AbschnittTest*

```
@Test
 public void nimmtWerteFuerStellenAuf() throws Exception {
   Abschnitt abschnitt = new Abschnitt();
   abschnitt.setName("abschnittsname");
   final String ersterWert = "a";
   final int ersteStelle = 1;
   final String zweiterWert = "b";
   final int zweiteStelle = 2;
   abschnitt.add(ersteStelle, ersterWert);
   abschnitt.add(zweiteStelle, zweiterWert);
   assertThat(ersterWert, is(abschnitt.findeWertAnStelle
                                              (ersteStelle)));
   assertThat(zweiterWert, is(abschnitt.findeWertAnStelle
                                             (zweiteStelle)));
 }
```

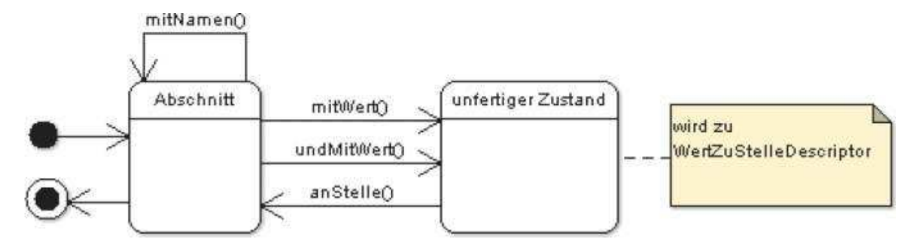
Listing 2: Erster Schritt zum Fluent Interface

```
public class Abschnitt {
  Map werteZuStellen = new HashMap();
  private String letzterWert;
  private String name;
  public Abschnitt mitWert(String wert) {
    return setLetzterWert(wert);
  }
  private Abschnitt setLetzterWert(String wert) {
    letzterWert = wert;
    return this;
  }
  public Abschnitt undMitWert(String wert) {
    return setLetzterWert(wert);
  }
  public Abschnitt anStelle(int stelle) {
    werteZuStellen.put(stelle, letzterWert);
    return this;
  }
  public String getName() {
    return name;
  }
  public static Abschnitt mitNamen(String name) {
    final Abschnitt abschnitt = new Abschnitt();
    abschnitt.name = name;
    return abschnitt;
  }

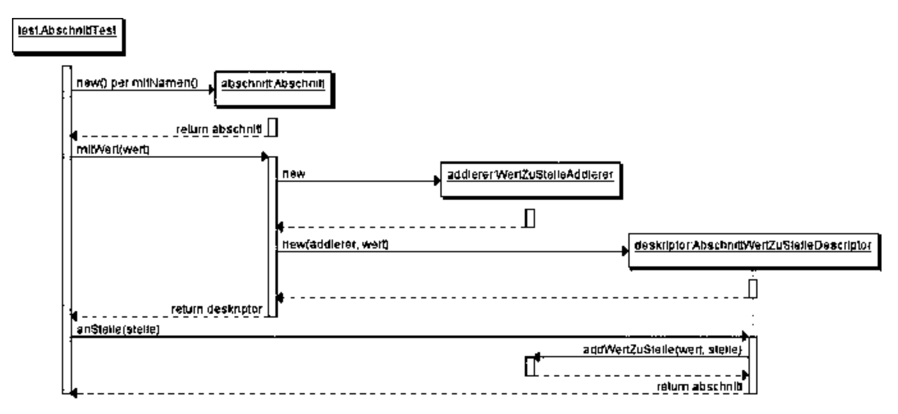
  /* weitere Methoden */
}
```


iX-TRACT

- Obwohl Entwurfsmuster wie „Erbauer“ (Builder) die Entwicklung einer Anwendung deutlich erleichtern können, verhindern sie nicht zwangsläufig unflexible oder inkonsistente Schnittstellen.
- Schnittstellendefinitionen, die sich wie umgangssprachliche Formulierungen lesen und einer internen Grammatik folgen, gewährleisten eine konsistente Objekterzeugung.
- Die Kombination des Builder Pattern mit einem sogenannten Fluent Interface erleichtert die Definition solcher Schnittstellen erheblich. Das Ergebnis dieser Kombination ist eine interne domänenspezifische Sprache.



Der Deskriptor verhindert, dass ein *Abschnitt* während seiner Konstruktion in einen unfertigen Zustand gerät (Abb. 1).



Die Implementierung auf Basis des Entwurfsmusters „Befehl“ bewirkt, dass *mitWert* nur die öffentlichen Methoden des Deskriptors aufrufen kann (Abb. 2).

thoden beliebig miteinander verknüpfbar sind, ist keine Konsistenz des konstruierten Objekts zu gewährleisten:

```
Abschnitt abschnitt =
    Abschnitt.mitNamen("abschnittsname")
    .mitWert("a").mitWert("b").anStelle(2);
```

Offensichtlich hat der Konstrukteur hier vergessen, den Wert *a* an die Stelle *1* zu schreiben. Das Verhalten dieses halbfertigen Objekts ist nicht ersichtlich, ohne den Quellcode der Abschnittsklasse zu studieren. Dies jedoch sollte wiederum für eine gute API unnötig sein; selbsterklärende Schnittstellen erhöhen ihre Benutzbarkeit enorm.

Leider konnte die zartschmelzende Variante die Unübersichtlichkeit der festen API nicht beseitigen. Hierzu ein Blick auf die Code-Vervollständigung: Eine IDE bietet bei der Code Completion auf eine Tastenkombination hin all die Codestücke wie Variablen, Methoden und Klassen an, die an der Stelle, an der sich der Cursor befindet, sinnvoll sind. Insbesondere dient dies dazu, an Objekten diejenigen Methoden ausfindig zu machen, die an ihm aufgerufen werden können. So lässt sich schnell durch eine API navigieren und Code niederschreiben.

Abschnitt mitNamen(String name) ist die einzige statische Methode, die durch Code-Vervollständigung an der Abschnittsklasse angeboten wird, sodass der Benutzer nichts falsch machen kann. Die zur Konstruktion von Abschnitten gedachten Objekt-Methoden dagegen sind *Abschnitt mitWert(String wert)*, *undMitWert(String wert)* sowie *Abschnitt anStelle(int stelle)*. Es ist jetzt für den Benutzer nicht ersichtlich, welche Methoden er aufrufen darf (*mitWert()* sowie *undMitWert()*) und welche nicht (*anStelle()*). Selbst die Reihenfolge der Code-Aufrufe könnte vertauscht werden: Statt *.mitWert("a").anStelle(1)* könnte der Entwickler *.anStelle(1). mitWert("a")* schreiben – und sich zu Recht wundern, warum er keinen brauchbaren Abschnitt erzeugen konnte. Hier hilft ihm auch die deutsche Grammatik nicht weiter, denn die Sätze „Abschnitt mit Wert a an Stelle 1“ und „Abschnitt an Stelle 1 mit Wert a“ folgen beide einem legitimen Satzbau.

Flüssige API muss Aufgaben delegieren

Diese beiden Einschränkungen – inkonsistente Objekterzeugung und unzureichende Vorgabe der Grammatik durch Code Completion – lassen diese Implementierung eines Abschnittes nicht flüssig, sondern eher zartschmelzend erscheinen.

Ein vollständiger Übergang in den flüssigen Aggregatzustand lässt sich durch eine Grammatik erreichen. Dies bedeutet, die Reihenfolge der erlaubten Methodenaufrufe zu analysieren und die Stellen zu identifizieren, die das zu konstruierende Objekt in einem inkonsistenten und damit unbrauchbaren Zustand hinterlassen. Ein Zustandsdiagramm hilft da weiter (Abbildung 1).

Der Einstieg in die Konstruktion erfolgt direkt bei der Klasse *Abschnitt*. Von hier aus kann die Methode *mitNamen()* aufgerufen werden und liefert einen konsistenten Abschnitt ohne Werte zurück. Die Methoden *mitWert()* sowie *undMitWert()* hingegen dürfen keinen Abschnitt zurückliefern. Bei ihrem Aufruf ist der Abschnitt in einem inkonsistenten und unfertigen Zustand. Erst ein weiterer Methodenaufruf von *anStelle()* liefert einen konsistenten Abschnitt.

Es kann viele unfertige Zustände während der Konstruktion eines Objektes mittels eines Fluent Interface geben. Sie zu identifizieren ist aber nur die halbe Miete; unfertige Zustände werden in sogenannten Deskriptoren implementiert. Durch den Einsatz eines Deskriptors muss die Abschnittsklasse nicht mehr sich selbst zurückgeben, wenn *mitWert()* oder *undMitWert()* an ihr aufgerufen wird. Der Benutzer erhält statt eines Objekts vom Typ *Abschnitt* eins vom Typ des Deskriptors. In diesem Fall soll er *WertZuStelleDescriptor* heißen. Der Benutzer kann jetzt nur noch die Methoden aufrufen, die der Deskriptor bereitstellt. Code wie der folgende würde nun nicht mehr kompilieren:

```
Abschnitt abschnitt =
    Abschnitt.mitNamen("abschnittsname")
    .mitWert("a").mitWert("b").anStelle(2);
```

Der erste Aufruf von *mitWert()* liefert einen Deskriptor zurück, an dem ein erneuter Aufruf von *mitWert()* nicht erlaubt ist. Somit kann das Programm nur noch konsistente Objekte erzeugen.

Zwar ist die Arbeit mit dem Descriptor-Entwurfsmuster gewöhnungsbedürftig, aber dafür flexibel ausbaubar. Deskriptoren können andere Deskriptoren zurückgeben und somit Grammatiken beliebiger Komplexität realisieren.

Ebenfalls gelöst durch den Einsatz von Deskriptoren ist die unzureichende Vorgabe der Grammatik durch Code Completion: Überall im Quellcode werden bei der Erzeugung des Abschnittes nur die Methoden angeboten, die der definierten Grammatik entsprechen. Den um den Einsatz von Deskriptoren modifizierten Abschnitt zeigt Listing 3.

Die deutlichste Änderung ist in der Methode *mitWert()* zu sehen: Durch

einen Callback-Aufruf mit dem Interface *WertZuStelleAddierer* wird anstelle eines *Abschnitt*s ein *AbschnittWertZuStelleDescriptor* zurückgegeben. Die Frage ist, warum hier eine anonyme Klasse zum Einsatz kommt, anstatt dass der Abschnitt dem Deskriptor gleich eine Referenz des zu konstruierenden Abschnitts, also sich selbst, übergibt. In der klassischen Implementierung eines Abschnitts gibt es eine Methode *add(String wert, int stelle)*, die der Deskriptor direkt aufrufen könnte.

Wenn der Deskriptor eine Referenz auf *Abschnitt* setzt, bedeutet das allerdings eine zyklische Abhängigkeit zwischen ihm und dem Abschnitt, ergo schlechtes Design. Aus Sicht des Fluent Interface gibt es noch einen pragmatischen Grund, dies zu vermeiden. Bei der Konstruktion des Objekts sollen keine Methoden mitwirken, die außerhalb der definierten Grammatik sind. *add()* wäre genau solch eine Methode. Ihren Aufruf verhindert das Interface *WertZuStelleAddierer*. Listing 4 zeigt den Code des Addierers und des Deskriptors.

Das Sequenzdiagramm in Abbildung 2 soll das verdeutlichen. Zunächst wird ein *Abschnitt* vom *Test mitNamen()* erzeugt. Für den Addierer gibt das Interface nur die Schnittstelle vor, und die dazugehörige anonyme Klasse bestimmt die Implementierung anhand des Entwurfmusters „Befehl“ (Command). Der Deskriptor nimmt den Addierer auf und ruft ihn zusammen mit dem Wert auf, sobald der Konstrukteur an der Abschnittsklasse *mitWert()* aufruft. Der Aufrufer hat dann nur noch die Möglichkeit, die öffentlichen Methoden des Deskriptors aufzurufen, also die nächsten grammatikalisch validen Schritte zu gehen. In diesem Fall ist dies die Methode *anStelle()* und der Rückgabewert ist wieder *Abschnitt*.

Dank der flüssigen Schnittstelle ist die Lesbarkeit des Codes nach wie vor gegeben, und die definierte Grammatik garantiert Flexibilität und Konsistenz. Darüber hinaus ist die API jetzt übersichtlich – allerdings nur für die Konstruktion. Nicht so gut steht es mit der weiteren Verwendung im Lebenszyklus des Objekts, denn an einem fertig konstruierten Objekt können nun folgende Methoden aufgerufen werden:

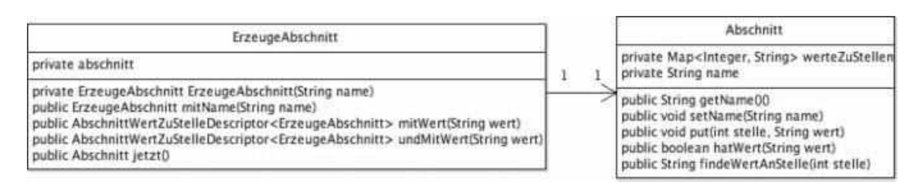
Listing 3: Erweiterung um einen Deskriptor

```
public class Abschnitt {
  private final Map werteZuStellen = new HashMap();
  private String name;
  public static Abschnitt mitNamen(String name) {
    Abschnitt abschnitt = new Abschnitt();
    abschnitt.name = name;
    return abschnitt;
  }
  public AbschnittWertZuStelleDescriptor mitWert(String wert) {
    final Abschnitt abschnitt = this;
    final WertZuStelleAddierer addierer = new WertZuStelleAddierer() {
      public Abschnitt addWertZuStelle(String wert, int stelle) {
        werteZuStellen.put(stelle, wert);
        return abschnitt;
      }
    };
    return new AbschnittWertZuStelleDescriptor(addierer, wert);
  }
  public AbschnittWertZuStelleDescriptor undMitWert(String wert) {
    return mitWert(wert);
  }
  public String getName() {
    return name;
  }
  /* weitere Methoden */
}
```

Listing 4: Addierer und Deskriptor

```
public class AbschnittWertZuStelleDescriptor {

  private WertZuStelleAddierer addierer;
  private String letzterWert;
  public AbschnittWertZuStelleDescriptor(WertZuStelleAddierer addierer,
      String letzterWert) {
    this.addierer = addierer;
    this.letzterWert = letzterWert;
  }
  public Rueckgabe anStelle(int stelle) {
    return addierer.addWertZuStelle(letzterWert, stelle);
  }
}
public interface WertZuStelleAddierer {
  Rueckgabewert addWertZuStelle(String wert, int stelle);
}
```



Der erzeugte *Abschnitt* beschränkt sich auf die Repräsentation und hat keine konstruierenden Methoden mehr (Abb. 3).

– *static Abschnitt mitNamen(String name)*
– *AbschnittWertZuStelleDescriptor mitWert(String wert)*
– *AbschnittWertZuStelleDescriptor undMitWert(String wert)*
– *String findeWertAnStelle(int stelle)*
– *boolean hatWert(String wert)*
– *String getName()*

Die ersten drei Methoden – die des Fluent Interface – dienen zur Konstruktion eines Abschnitts und werden am fertig gebauten Objekt nicht mehr benötigt. Hier sind Methoden mit entsprechender Logik gefragt, wie sie bei den beiden nächsten Methoden gegeben ist, oder abfragende Methoden wie die letzte. Schließlich bleibt die Frage offen: Wie kann man einem fertigen Objekt später ein weiteres Stelle-Wert-Paar hinzufügen? Das wäre über die Methoden des Fluent Interface möglich, allerdings drücken solche Satzfetzen nicht mehr aus, was sie tun:

```
abschnitt.mitWert("weiterer wert").anStelle(5);
```

Methoden zur Konstruktion eigenen sich nicht zur späteren Manipulation eines Objekts. Hinzu kommt, dass die Abschnittsklasse zwei Aufgaben gleichzeitig übernimmt: die Konstruktion eines komplexen Datentyps (sich selbst) sowie die Datenhaltung samt Logik. Dies aber widerspricht dem Prinzip des „Separation of Concerns“ (SoC) [d], das besagt, dass eine Klasse nur eine Aufgabe erfüllen sollte.

Flüssiger Erbauer trennt Belange

Die Rettung naht in Form des Erzeugungsmusters „Erbauer“ (Builder). Ein Erbauer trennt die Repräsentation eines Objekts von seiner Konstruktion, in diesem Falle die konstruierenden Methoden (und wofür sie stehen) vom Rest des Abschnitts. Ein Erbauer in Kombination mit einer flüssigen Schnittstelle, von Fowler „Expression Builder“ [e] genannt, ist eine deutliche Bereicherung im Hinblick auf die Lesbarkeit:

```
Abschnitt abschnitt =
  ErzeugeAbschnitt.mitNamen("abschnittsname").
  mitWert("a").anStelle(1).
  undMitWert("b").anStelle(2).jetzt();
```

Zuerst fällt auf, dass der Erbauer selbst mit einem Verb statt mit einem Nomen benannt ist. Dieser Kniff [f] lässt nun einen vollständigen Satz im Imperativ entstehen:

„Erzeuge Abschnitt mit Namen *abschnittsname* mit Wert *a* an Stelle *1* und mit Wert *b* an Stelle *2*, jetzt!

Zurück gibt der Flüssige Erbauer ein Objekt vom Typ *Abschnitt*, der keine konstruierenden Methoden mehr hat und sich ganz um die Repräsentation seiner selbst kümmern kann. Abbildung 3 zeigt die API der Klassen *ErzeugeAbschnitt* und *Abschnitt*.

An dieser Stelle lässt sich einwenden, dass noch kein Separation of Concerns stattgefunden hat. Immerhin gibt es ja noch Methoden wie *setName(String name)* und *put(int Stelle, String wert)*. Doch hier ist zu unterscheiden zwischen konstruierenden und verändernden Methoden. Alle konstruierenden sind jetzt am Builder verankert. Ob das Objekt nach der Konstruktion noch veränderbar sein darf, ist eine Designentscheidung, die unabhängig von der Konstruktion ist. In diesem Fall ist die Entscheidung für ein veränderliches Objekt gefallen; unveränderliche Objekte hätten keine solchen modifizierenden Methoden.

Eine Besonderheit stellt die Methode *jetzt()* an der Erbauer-Klasse *ErzeugeAbschnitt* dar. Prinzipiell könnte man einem *Abschnitt* beliebig viele Werte hinzufügen. Hierzu muss stets der Erbauer herhalten, und so gibt jede Methode, die einen Wert für eine Stelle aufnimmt, letztendlich ein Objekt vom Typ *ErzeugeAbschnitt* zurück. Will man jedoch keinen Wert mehr hinzufügen, soll der Rückgabewert ein *Abschnitt* sein. Dies erreicht der Aufruf von *jetzt()*, der den Verantwortungsbereich des flüssigen Erbauers terminiert. Von hier an ist der *Abschnitt* auf sich allein gestellt. (Ein lauffähiges Beispiel ist über den *iX*-Listingservice erhältlich.)

Fazit

Durch evolutionäres Design getriebenen entwickelte sich aus einer „festen API“, die unlesbar, unflexibel, unübersichtlich und inkonsistent war, zunächst eine „zartschmelzende API“. Diese war jedoch unübersichtlich aufgrund eines naiven Entwurfes, der keine Grammatik berücksichtigte, und ermöglichte eine inkonsistente Objekterzeugung. Hieraus entwickelte sich ein Objekt mit einer „flüssigen Schnittstelle“, das eine Grammatik vorgegeben hat und damit eine konsistente Objekterzeugung gewährleistete. Lediglich die Übersichtlichkeit bei der Betrachtung der Objektschnittstelle war noch verbesserungsbedürftig. Hierfür sorgte der letzte Schritt in der Evolution des Beispiels: der „flüssige Erbauer“. (ka)

BERND SCHIFFER

ist Senior Softwareentwickler bei der akquinet it-agile GmbH Hamburg.

[1] Eric Evans; Domain-driven Design; Tackling Complexity in the Heart of Software; Addison-Wesley, 2004

Onlinequellen

[a] Martin Fowler: FluentInterface
www.martinfowler.com/bliki/FluentInterface.html

[b] Martin Fowler: DomainSpecificLanguage
www.martinfowler.com/bliki/DomainSpecificLanguage.html

[c] Martin Fowler: Language Workbenches; The Killer-App for Domain Specific Languages?
www.martinfowler.com/articles/languageWorkbench.html

[d] Wikipedia: Separation of Concerns
en.wikipedia.org/wiki/Separation_of_concerns

[e] Martin Fowler: ExpressionBuilder
www.martinfowler.com/bliki/ExpressionBuilder.html

[f] Anders Norås: I’m coming down with a serious case of the DSLs!
andersnoras.com/blogs/anoras/archive/2007/07/04/i-m-coming-down-with-a-serious-case-of-the-dsls.aspx



Entwicklung mit dem iPhone SDK

Ein bisschen Freiheit

Markus Stäuble

Das iPhone hat zwar großes Potenzial. Um weitere Kunden zu gewinnen, braucht Apple jedoch mehr Anwendungen. Diesen Bedarf soll das vor Kurzem veröffentlichte iPhone SDK decken, indem es Entwickler für das Gerät motiviert.

Endbenutzer nahmen Apples Produkte jahrelang höchstens als Designgegenstand wahr. Dies hat sich unter anderem durch den iPod und die Vielfalt seiner Modelle schlagartig verändert. Er hat vielen gezeigt, dass Apple nicht nur schöne, sondern auch einfach zu bedienende Geräte herstellen kann. Das motivierte etliche iPod-Besitzer, es einmal mit einem Mac zu versuchen. Einen ähnlichen Effekt wie bei den Endbenutzern möchte Apple nun via iPhone bei Unternehmenskunden erreichen. Hier gilt es vor allem, einen Konkurrenten zu verdrängen: den Blackberry.

Ein wichtiger Schritt dahin war die Lizenzierung von Microsofts Activesync für Exchange und seine Integration in die kommende Version 2.0 des iPhone-Betriebssystems. Sie soll als kostenloses Firmware-Update Ende Juni 2008 zu Verfügung stehen. Activesync kann dem Telefon per Push beispielsweise die E-Mails, Kontakte und Termine vom Exchange-Server schicken (siehe www.apple.com/de/iphone/enterprise/) – eine Fähigkeit, die für viele Unternehmen kaufentscheidend sein dürfte. Mit dem Anfang März veröffentlichten SDK können Firmen nun erstmals nicht nur Webprogramme, sondern native iPhone-Anwendungen erstellen. Mit der Publizierung des iPhone SDK stellte KPCB (Kleiner Perkins Caufield & Byers) 100 Millionen US-Dollar als Risikokapital „iFund“ zur Verfügung (siehe Onlinequellen [a]). Es soll Anreiz für Entwickler und Unternehmen sein, sich eine Existenz mit der Entwicklung von Applikationen für iPhone oder iPod touch aufzubauen.

Ein großes Paket nur für Mitglieder

Erster Schritt zur Entwicklung einer eigenen Anwendung mit dem neuen iPhone SDK ist die kostenlose Mitgliedschaft bei der Apple Developer Connection (ADC), ohne die der Download des SDK und somit eine Entwicklung nicht möglich ist. Beim Herunterladen dürfte viele die Größe des Pakets (2,1 GByte für die Beta 1 und immer noch 1,36 GByte für die Beta 2) allerdings förmlich erschlagen.

Für die Dokumentation steht immerhin ein Aktualisierungsdienst zur Verfügung, und da sich derzeit viel ändert, empfiehlt sich seine tägliche Nutzung. Neben dem reinen Softwarepaket bietet ADC zahlreiche Dokumentationen, unter anderem Videos, die es auch kostenlos via iTunes gibt. Vor allem die Code-Beispiele helfen beim Einstieg in die iPhone/iPod-touch-Entwicklung.

Auf dem iPhone und dem iPod touch läuft eine Variante von Mac OS X. Deshalb erfolgt die Programmierung einer Applikation für diese Geräte wie bei einem herkömmlichen Mac in der Programmiersprache Objective-C, ein mit Smalltalk-ähnlicher Objektorientierung aufgepepptes C.

Für viele Entwickler bedeutet diese Sprache Neuland, das sie zunächst gründlich erkunden müssen. Einen Einblick in die Syntax von Objective-C gibt es beim ADC [c]. Neben der reinen Syntax ist vor allem für Java- und .Net-Programmierer wichtig, dass Objective-C keinen Garbage Collector kennt, sondern dass sie sich selbst um das Aufräumen nicht mehr benötigter Ressourcen kümmern müssen – wie in C und C++. Das Framework zur Anwendungsentwicklung nennt sich Cocoa Touch, analog zu Cocoa für Mac

iX-TRACT

- Mit einem SDK für das iPhone und den iPod touch sollen Entwickler eigene Anwendungen für die Geräte erstellen können. Damit verabschiedet sich Apple davon, nur Webanwendungen darauf zuzulassen.
- Die Erstellung von iPhone-Programmen erfolgt mit derselben IDE wie für Mac-Software. Auch die Programmiersprache Objective-C ist identisch.
- Drittanbieter können ihre Anwendungen nur über den iTunes-Shop vertreiben und müssen ihre Einnahmen mit Apple teilen.

OS X. Es ist die oberste Schicht innerhalb des iPhone OS; darunter liegen Media, Core Services und Core OS. Bei der Entwicklung sollte man Methoden aus höher liegenden Schichten bevorzugen, also am besten aus Cocoa Touch.

Neue, alte Entwicklungsumgebung

Da das iPhone das Framework Cocoa Touch verwendet, lag es nahe, die für Mac OS X eingesetzte IDE *XCode* zu benutzen. Sie enthält alle notwendigen Funktionen einer ausgewachsenen Entwicklungsumgebung.

XCode bietet folgende Möglichkeiten:
– iPhone-Verwaltung mit dem *Organizer*: Installation, Aktualisieren und Entfernen von Anwendungen auf dem iPhone;
– Entwicklung des Codes;
– Übersetzen und Erzeugen der Anwendung für die Installation;
– Hilfe bei der Fehlersuche in der Anwendung, unabhängig davon, ob sie im Simulator oder auf dem Gerät läuft;
– Analysen mit *Instruments*, unter anderem Performance-Analysen;
– Unterstützung durch Onlinehilfe und Code-Vervollständigung.

Anhand einer einfachen To-do-Liste zur Verwaltung von Aufgaben sei kurz skizziert, welche Schritte notwendig sind, um eine eigene Anwendung zu erstellen. Der Code steht auf dem *iX*-Listingserver zum Herunterladen bereit. Den besten Start ins Programmieren für das iPhone bildet eins der von Apple mitgelieferten Beispiele. Dadurch ist der notwendige Infrastrukturrahmen vorhanden. Falls man unbedingt direkt auf der grünen Wiese eine Applikation entwickeln möchte, empfiehlt es sich in XCode über „File -> New Project -> Cocoa Touch Application“ das Grundgerüst zu erstellen.

Die To-do-Liste soll das Eingeben und Ändern von Aufgaben erlauben, sie in einer Liste anzeigen (überfällige in einer anderen Farbe) und eine Funktion zum Löschen erledigter Aufgaben bieten (siehe Abb. 1). Die Daten selbst speichert die SQL-Datenbank *SQLite*. Ausgangspunkt für diese Anwendung war das von Apple zur Verfügung gestellte *SQLiteBooks*.

Eine wesentliche Aufgabe bei der Entwicklung einer iPhone-Applikation ist das Gestalten der Oberfläche. Hierfür waren mit der Beta 1 des SDK noch mühsame Arbeiten direkt im Quellcode nötig. Größte Änderung der Ende März veröffentlichen Beta 2 ist der dort mitgelieferte grafische Interfacebuilder (siehe Abb. 2).

Ein Fenster pro Anwendung

Wichtig bei der Gestaltung von Oberflächen für das iPhone ist, dass Anwendungen hauptsächlich aus einem Applikationsfenster (Basisklasse für alle Fenster ist *UIView*) bestehen, das Elemente wie die Navigationsleiste aufnehmen kann.

Zur Ablaufsteuerung innerhalb der Applikation dienen Events in den Controller-Klassen. Die GUI-Elemente liegen wie in einem Stapel aufeinander und bilden die sogenannte View Hierarchy. Ein Button der Navigationsleiste liegt darin über ihr. Löst der Benutzer ein Ereignis aus, sendet das Framework es zunächst an das oberste Element der View Hierachy. Wenn dieses den Event nicht verarbeitet, erreicht er das darunterliegende Element – und so weiter, bis er an der Wurzel anlangt.

Für die Gestaltung der Oberflächen stehen folgende Typen von Views zur Verfügung:
– Windows: Ein Window ist immer das niedrigste Element in der View Hierarchie, quasi die Wurzel.
– Toolbars: Eine Toolbar erscheint am unteren Rand der Bedienoberfläche.
– Navigationbars: Eine Navigationsleiste erscheint am oberen Rand der Bedienoberfläche.

Listing 1: AppDelegate.m

```
- (void)applicationDidFinishLaunching:(UIApplication *)application {
    [self createEditableCopyOfDatabaseIfNeeded];
   // Initialisierung der Datenbank (SQLLite)
   [self initializeDatabase];
   // Hauptfenster erzeugen
   window = [[UIWindow alloc] initWithFrame:[[UIScreen mainScreen] bounds]];
   // Initialisierung table view controller
   masterViewController = [[MasterViewController alloc] init];
   // NavigationController erzeugen
   navigationController = [[UINavigationController alloc] ↙
                              initWithRootViewController:masterViewController];
   // Den View des Navigation Controllers zum Hauptfenster hinzufügen
   [window addSubview:[navigationController view]];
   [window makeKeyAndVisible];
}
```

Nach dem Start, jedoch bevor etwas auf dem Display zu sehen ist: Eine Methode des Delegate baut den View der Anwendung auf.



Eingabe einer neuen Aufgabe für die To-do-Liste im iPhone-Simulator. Für die Eingabe stehen die iPhone-typischen Elemente zur Verfügung (Abb. 1).

Beim Verzicht auf zusätzliche Elemente wie eine Navigations- oder eine Werkzeugleiste reicht die Basisklasse *UIView* meistens aus. Sie stammt von *UIResponder* ab und bietet somit Methoden für die Verarbeitung von Benutzer-Events. Zur Gestaltung des GUI stellt das SDK weitere Elemente bereit:
– Container wie *UIScrollView* (Ergänzung um einen Rollbalken);
– Elemente vom Typ *UIControl*;
– Dialoge und Informationsanzeigen (unter anderem *UIModalView*);
– Elemente zur Darstellung von formatiertem Text oder Webinhalten wie *UIWebView*.

Für Applikationen mit mehreren Views (zum Beispiel bei der Verwendung einer Toolbar) sieht das Framework den Einsatz eines *ViewController* vor, der Methoden zur Verwaltung anderer Objekte bietet. Unter anderem kann er die automatische Neuorientierung der Oberfläche übernehmen, wenn der Anwender sein iPhone dreht.

Zum Starten der Anwendung erzeugt der Programmierer eine Instanz von *UIApplicationMain*. Sie bekommt als Parameter einen sogenannten Delegate mitgegeben, der nicht von einer bestimmten

Klasse abstammt, sondern das *UIApplicationDelegateProtocol* implementiert. Der Unterschied zu einem reinen Interface besteht darin, dass die jeweilige Klasse nicht alle Methoden bereitstellen muss. Der Delegate ähnelt also einem Hook: Vorhandene Methoden ruft das Framework gegebenenfalls auf, und nicht implementierte stören es nicht.

Eine wichtige optionale Methode des Delegate ist *applicationDidFinishLaunching()*. Ist sie vorhanden, ruft das Framework sie als Erstes nach dem Start auf – noch bevor die Anwendung auf dem Bildschirm erscheint. Hier ist es empfehlenswert, den View zusammenzusetzen, (vgl. den Aufruf von *addSubview()* in Listing 1). Hat man die Oberfläche mit dem Interface Builder erstellt, entfällt dieses Zusammensetzen des View. Stattdessen lädt man in *applicationDidFinishLaunching()* die vom Builder erzeugte *.xib*-Datei mit einer Beschreibung der Oberfläche im XML-Format.

iPhone-Anwendungen laufen innerhalb einer Application Sandbox, nur in diesem Bereich dürfen sie schreiben. Eine solche Sandkiste besteht aus der Applikation (dem Application Bundle), dem Verzeichnis *Documents* (Speicherort für Applikationsdaten), dem Verzeichnis *Library/Preferences* (Konfigurationsdaten, die die CFPreferences-API verwaltet) und einem temporären Verzeichnis *tmp*. Um das Aufräumen in Letzterem muss sich der Entwickler selber kümmern, denn einen Automatismus gibt es nicht. Die Anwendung innerhalb des Application Bundle besteht neben den Klassen aus Resource-Dateien, beispielsweise Bildern oder Texten für die Internationalisierung. Wichtig ist außerdem die Datei *Info.plist*, die die Anwendung beschreibt. Sie legt unter anderem fest, welches Icon das iPhone anzeigt.

Testen für Europäer nur im Simulator

Einen ersten Dämpfer bekamen Entwickler bei der Veröffentlichung des iPhone SDK verpasst: Sie können ihre Anwendungen nicht einfach auf das eigene iPhone laden und dort testen. Ein Test der entwickelten Anwendung mit dem iPhone SDK ist zunächst nur im Simulator möglich. Für die Installation auf einem iPhone oder iPod touch ist ein digitales Zertifikat erforderlich, das es nur im kostenpflichtigen iPhone Developer Program gibt (derzeit 99 US-$ pro Jahr für Entwickler, 299 US-$ für



Einfacher als direkt im Quellcode lassen sich die Oberflächen grafisch erstellen. Der Interface Builder ermöglicht zudem, sie direkt zu testen (Abb. 2).

interne Anwendungen eines Unternehmens). Selbst wer bereit ist, die Kosten zu tragen, muss sich als Europäer zunächst gedulden, denn an dem Programm dürfen bislang nur US-Bürger und -Firmen teilnehmen. Zur Verteilung von Drittsoftware will Apple seinen iTunes-Dienst nutzen. Entwickler bestimmen selbst den Preis für ihr Produkt. 70 % der Einnahmen erhalten sie, den Rest Apple. Bevor der Hersteller ein Programm in seinen Shop aufnimmt, will er es nach eigenem Bekunden prüfen.

Zu den finanziellen Hürden kommen technische Restriktionen, die Apple dem Entwickler auferlegt. So ist es nicht erlaubt, Hintergrundprozesse auszuführen und interpretierten Code in der Anwendung zu verwenden – es sei denn, er läuft in einem von der Laufzeitumgebung zur Verfügung gestellten Interpreter. Dadurch ist eine Java-VM auf dem iPhone in weite Ferne gerückt. Diese Restriktionen werden einerseits durch die Lizenzbestimmungen des iPhone SDK und andererseits durch das besagte iPhone Developer Program definiert. Apple versucht mit diesen Vorgaben vermutlich, die Stabilität der Plattform „iPhone“ zu gewährleisten und nicht Tür und Tor für schadhaften Code zu öffnen.

Es gibt viele Unterschiede zwischen Googles Android und dem iPhone SDK und darunter auch Gründe, weswegen Entwickler die eine oder andere Plattform wählen. Eine Rolle könnte die eingesetzte Programmiersprache spielen: Einem Java-Kenner ist Android näher als das Objective-C im iPhone. Apple hat auf seiner Seite zunächst die Entwickler, die ohnehin bereits mit XCode in Objective-C arbeiten. Jene, die noch keine Erfahrungen mit dem Mac und Objective-C gesammelt haben, werden sich jedoch erst einmal einarbeiten müssen.

Hier ist es an Apple, die auf seinen Webseiten angebotenen Informationen auszubauen und aktuell zu halten, um Frustrationen bei neuen Entwicklern zu vermeiden. Im Weg steht noch die Barriere des iPhone Developer Program, die Apple kaum beseitigen wird. Umso wichtiger, dass die Firma in der Entwicklergemeinde um Verständnis dafür wirbt.

Als größtes Hindernis für das Gewinnen neuer Programmierer könnte sich herausstellen, dass sie auf einem Mac arbeiten müssen – das verlangen die Lizenzbestimmungen. Damit dürfte Apple weniger Hobbyentwickler anziehen als Android oder andere Plattformen. Andererseits könnten die von iFund angebotenen Mittel einige reizen. Es bleibt sicherlich spannend, und am Ende wird wohl die Kombination aus Plattform und verfügbaren nützlichen Anwendungen die Gunst der meisten Anwender für sich gewinnen. (ck)

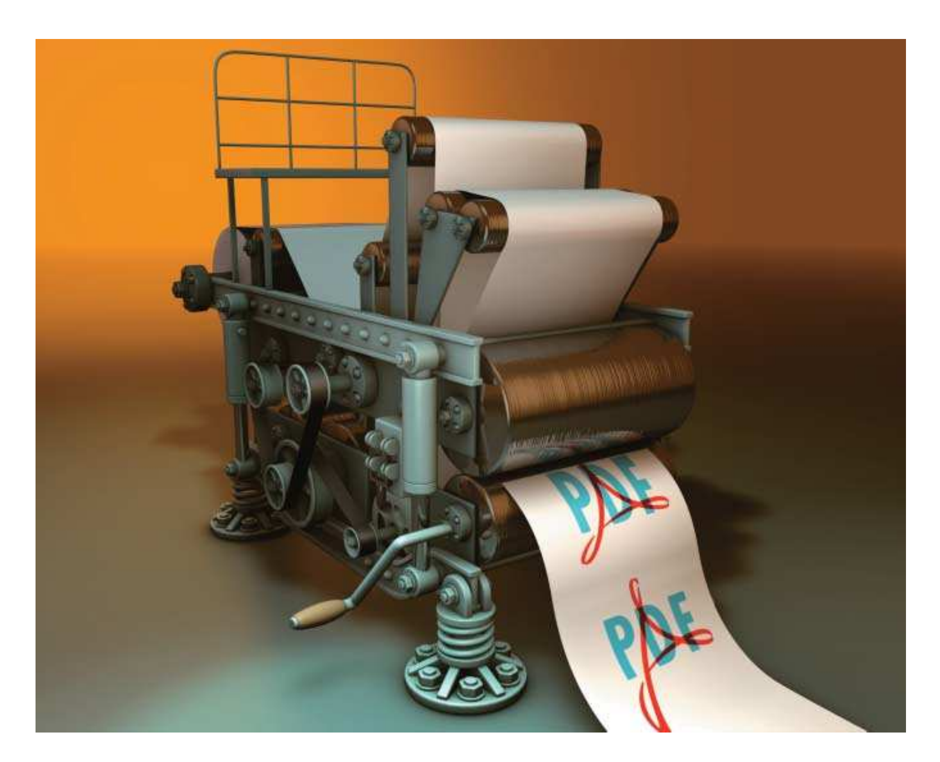
MARKUS STÄUBLE

ist Senior Software Engineer bei der namics (deutschland) GmbH. Schwerpunkte seiner Arbeit sind Projektleitung, Coaching, die Architektur von JavaEE-Anwendungen und deren Qualitätssicherung.



Onlinequellen

[a] iFund	http://www.kpcb.com/initiatives/ifund/index.html
[b] Apple Developer Connection	http://developer.apple.com/iphone
[c] Einstieg in Objective-C	http://developer.apple.com/iphone/gettingstarted/docs/objectivecprimer.action



PDF generieren mit dem Zend-PHP-Framework

Zeichenzauberer

Markus Bach

Anfang des Jahres hat Zend die neueste Version des hauseigenen PHP-Framework offiziell freigegeben. Es stellt neben einer umfangreichen Sammlung von Bibliotheken für High-Level-Dienste eine API zum Erstellen und Bearbeiten von PDFs zur Verfügung.

In den Anfängen von PHP war es einigermaßen mühsam, PDFs dynamisch zu erstellen. Und zwar war das Schlimme der initiale Aufwand, bis der Rahmen stand, um überhaupt ein erstes Dokument erstellen zu können. Man konnte externe Bibliotheken verwenden. Allerdings waren die meist nicht in PHP, sondern in C programmiert und mussten erst einkompiliert werden. Für erfahrene PHP-Administratoren zwar machbar, unerfahrene Anwender konnte es aber zum Aufgeben bringen. Zudem gab es in Shared-Hosting-Umgebungen meist nicht die Option, etwas an der PHP-Installation zu ändern, da diese in der Hoheit des Hosters lag.

Das hier behandelte Zend-Framework dagegen ist vollständig in PHP implementiert, was auch den wesentlichen Unterschied zu Lösungen wie 2004 in *iX* beschrieben [1] ausmacht. Das bedeutet, dass PHP in seiner Grundinstallation – Version 5.1.4 oder neuer – nicht geändert werden muss, außerdem sind auf dem Server keine weiteren Programme oder Bibliotheken erforderlich. Es müssen nur die Dateien des Framework vorhanden und im Zugriff sein. Die jeweils aktuelle Version findet sich auf der Projekt-Homepage [a]. Damit das Framework funktioniert, muss es in einem Pfad liegen, der in der Konfigurationsdirektive *include_path* enthalten ist. Wie man diese gegebenenfalls ändern kann, ist auf der PHP-Site (siehe Onlinequellen [c]) dokumentiert. Wichtig ist, dass man das Verzeichnis *library* unter dem Verzeichnisnamen des eingespielten Pakets in den Pfad aufnimmt, etwa *./ZendFramework-1.5.0/library*.

Diese Schritte vorausgesetzt, lädt folgender Code im PHP-Programm die Zend-API:

```
<?php
  require_once(‚Zend/Pdf.php');
?>
```

Das Zend-Framework unterstützt den PDF-Standard in der Version 1.4, entsprechend Adobes Acrobat 5. In den Dokumenten lassen sich Seiten hinzufügen oder entfernen, außerdem kann man die Sortierung und Dokumenteigenschaften (Autor, Titel, …) ändern. In die Dokumente lassen sich Texte, einfache Grafikelemente (Linien, Rechtecke, Polygone, Kreise und Ellipsen) sowie Bilder im JPG-, PNG- oder TIFF-Format zeichnen.

Dokumente erzeugen, öffnen und speichern

Objekte der Klasse *Zend_Pdf* repräsentieren Dokumente, deshalb kann das Erstellen und Laden über den Konstruktor oder durch statische Methoden erfolgen, die sich entweder auf den Pfad zu einer PDF-Datei oder das komplette Dokument in einer String-Variablen beziehen:

```
<?php
// Neues PDF erzeugen
$pdf1 = new Zend_Pdf();
// PDF-Datei laden
$pdf2 = Zend_Pdf::load($pathToPdf);
// Dokument aus einem String erzeugen
$pdf3 = Zend_Pdf::parse($pdfAsString);
?>
```

Um Änderungen im PDF-Dokument zu speichern, können Entwickler die Methoden *save* und *render* nutzen. Der Unterschied: *save* schreibt das Dokument in eine Datei, *render* gibt es als String zurück – etwa wenn es gleich zur Darstellung an einen Browser als Response geschickt werden soll:

```
<?php
// PDF in Datei speichern
$pdf->save($pathToPdf);
// PDF erzeugen und an Browser schicken
$pdfAsString = $pdf->render();
header(‚Content-type: application/pdf');
header(‚Content-Disposition: attachment; ⏎
                              filename=\"zend.pdf\"');
echo $pdfAsString;
?>
```

Die Metadaten eines Dokuments sind nicht Teil des Inhalts, sie dienen vielmehr dazu, Informationen zum Dokument selbst anzugeben. Folgende Attribute können optional ausgewertet und gesetzt werden:

Listing 1

```
<?php
// Style für Überschriften festlegen
$headlineStyle = new Zend_Pdf_Style();
$headlineStyle->setFont(Zend_Pdf_Font::fontWithName(Zend_Pdf_Font::FONT_HELVETICA_BOLD), 14);
$headlineStyle->setFillColor(new Zend_Pdf_Color_Html(‚#ff0000'));
// Style für Text festlegen
$bodyStyle = new Zend_Pdf_Style();
$bodyStyle->setFont(Zend_Pdf_Font::fontWithName(Zend_Pdf_Font::FONT_HELVETICA), 10);
$bodyStyle->setFillColor(new Zend_Pdf_Color_Rgb(0, 0, 0.9));
// Style setzen und Überschrift schreiben:
$page->setStyle($headlineStyle);
$page->drawText(‚Überschrift', 10, 500);
// Style setzen und Body schreiben:
$page->setStyle($bodyStyle);
$page->drawText(‚Text Text Text', 10, 450);
?>
```

– *Title*: Titel des Dokuments
– *Author*: Name des Erstellers
– *Subject*: kurze Beschreibung des Inhalts
– *Creator* und *Producer*: Angaben darüber, mit welchen Anwendungen das Dokument erstellt beziehungsweise mit welcher Anwendung das Rohdokument in PDF konvertiert wurde
– *CreationDate*: Datum der Erzeugung des Dokuments im Format D:YYYY MMDDHHmm wobei D: konstant ist und die restlichen Parameter denen der PHP-Funktion *date* entsprechen
– *ModDate*: Datum der letzten Änderung, das Format entspricht dem von *CreationDate*

Die einzelnen Attribute liegen im PDF-Objekt als assoziatives Array vor und sind über die Schlüsselwörter einfach ansprechbar:

```
<?php
$oldAuthor = $pdf->properties[‚Author'];
$pdf->properties[‚Author'] = $oldAuthor .", ↵
                                    Weiterer Autor";
?>
```

PDF-Dokumente sind seitenorientiert aufgebaut, das heißt, alle Seiten bestehen unabhängig voneinander und sind deshalb einzeln änderbar. Anders formatierte Seiten als schon im Dokument vorhandene lassen sich einfügen. Innerhalb der API repräsentiert die Klasse *Zend_Pdf_Page* Seiten im Dokument. Organisiert sind sie innerhalb der Objekte vom Typ *Zend_Pdf* als öffentliches Array, deshalb lassen sich Seiten leicht ansprechen, entfernen, umsortieren und mit allen Array-Funktionen bearbeiten:

```
<?php
// 5. Seite des Dokuments laden
$pageFive = $pdf->pages[4];
// 10. Seite entfernen
unset($pdf->pages[9]);
// 5. und 6. Seite vertauschen
$pdf->pages[4] = $pdf->pages[5];
$pdf->pages[5] = $pageFive;
// Seiten verwürfeln
shuffle($pdf->pages);
?>
```

Neue Seiten lassen sich auf zwei Arten zu einem Dokument hinzufügen: Zum einen über die statische Methode *newPage* der Klasse *Zend_Pdf*, zum anderen über den Konstruktor der Klasse *Zend_Pdf_Page*. Der Unterschied ist, dass *newPage* eine schon gebundene Seite erzeugt und der Konstruktor eine ungebundene. Jedoch müssen beide Seiten dem *Page*-Array des PDF-Objekts explizit zugewiesen werden, damit sie Teil des Dokuments sind. Ungebundene Seiten kann man in mehrere PDF-Objekte eingefügen, ohne sie neu erstellen zu müssen. Dies ist nützlich, wenn eine Seite als Vorlage für mehrere gleichartige Seiten dienen soll.

```
<?php
// Gebundene Seite einfügen
$pageBound = $pdf1-
>newPage(Zend_Pdf_Page::SIZE_A4);
$pdf1->pages[] = $pageBound;
// Ungebundene Seite erzeugen
$pageUnbound = new
Zend_Pdf_Page(Zend_Pdf_Page::SIZE_A4);
// Seite an zwei unabhängige PDFs anhängen
$pdf1->pages[] = $pageUnbound;
$pdf2->pages[] = $pageUnbound;
?>
```

Die Methode *newPage* und der Konstruktor erwarten jeweils als Parameter die Seitengröße, als Konstanten sind die Felder *SIZE_A4, SIZE_A4_ LANDSCAPE, SIZE_LETTER* oder *SIZE_LETTER_LANDSCAPE* der Klasse *Zend_Pdf_Page* verwendbar. Die Seitengröße kann man auch selbst definieren, indem man Höhe und Breite in Pixel als Parameter übergibt.

Um eine bestehende Seite als Vorlage für eine neue Seite zu verwenden, übergibt man die Template-Seite dem Konstruktor, der so eine ungebundene Seite erstellt, die sich dem PDF wieder anhängen lässt:

```
<?php
// 1. Seite des Dokuments als Template laden
$templatePage = $pdf->pages[0];
// Neue Seite mit dem Template erzeugen
$newPage = new Zend_Pdf_Page($templatePage);
// Neue Seite hinzufügen
$pdf->pages[] = $newPage;
?>
```

Da jetzt die Grundlagen geschaffen sind, um mit Dokumenten umzugehen,

Listing 2

```
<?php // Zunächst wird der Style definiert $style = new Zend_Pdf_Style(); $style->setFillColor
(new Zend_Pdf_Color_Html('#ff0000')); $style->setLineColor(new Zend_Pdf_Color_Html
('#00ff00')); $style->setLineWidth(3); $page->setStyle($style);
// Zeichne einen Kreis an // Position x = 50 und y = 300 mit Radius 30 Pixel $page->drawCircle
(50, 300, 30);
// Zeichne ein Kreissegment // von Winkel PI/4 bis 3*PI/4 $page->drawCircle(100, 300, 30,
(M_PI / 4), (3 * M_PI / 4));
// Zeichne ein gefülltes Rechteck mit Außenlinie mit den Koordinaten
// der Eckpunkte 100 / 300 und 200 / 400 $page->drawRectangle(100, 300, 200, 400,
Zend_Pdf_Page::SHAPE_DRAW_FILL_AND_STROKE);
// Zeichne nur die Außenlinie $page->drawRectangle(300, 300, 400, 400,
Zend_Pdf_Page::SHAPE_DRAW_STROKE);
// Zeichne nur die Füllung $page->drawRectangle(100, 100, 200, 200,
Zend_Pdf_Page::SHAPE_DRAW_FILL); ?>
```

können die Seiten mit Inhalt gefüllt werden. Um einen Text einzufügen, verwendet man die Methode *drawText* der Klasse *Zend_Pdf_Page*. Sie erwartet als Parameter den Text und die Position des Textes als XY-Koordinaten (Nullpunkt in der linken unteren Ecke). Optional kann man das Encoding des Textes angeben, falls es zu Problemen mit Sonderzeichen kommt:

```
<?php
$page = new Zend_Pdf_Page(Zend_Pdf_Page:: ⁊
                                    SIZE_A4);
// Text in Latin1-Codierung schreiben
$page->drawText('Hello PDF world!', 100, 100,
'Latin1');
?>
```

Leider geben diese Code-Zeilen nur eine Fehlermeldung aus, denn es ist nur festgelegt, was und wo dargestellt werden soll, aber es fehlen Angaben über Schriftart, -stil und -farbe, die in Objekten der Klasse *Zend_Pdf_Style* stehen. Pro PDF können mehrere Styles zum Einsatz kommen, jeweils gesetzt vor dem Aufruf der *draw*-Methoden. Ein Style bleibt solange gültig, bis ein neuer angegeben wird. Ein Beispiel zeigt Listing 1 (ein Beispielprogramm mit – fast – allen besprochene Befehlen ist über den *iX*-Listing-Service erhältlich. [d]

Texte, Schriftarten und Farben

Schriftart und Schriftgröße werden dem Style mit der Methode *setFont* zugewiesen, wobei Schriftarten mit statischen Methoden der Klasse *Zend_Pdf_Font* zunächst zu laden sind. Das Framework definiert bereits sechs Schriftarten, ladbar über ihren Namen. *Zend_Pdf_Font* enthält zum einfachen Umgang entsprechende Konstanten. Andere Schriftarten können über *fontWithPath* aus einer Datei mit der Truetype-Definition geladen werden.

Die Schriftfarbe legt *setFillColor* fest, mit einem Farb-Objekt als Parameter. Die Farb-Objekte lassen sich auf vier verschiedene Arten definieren. Der Konstruktor der Klasse *Zend_Pdf_Color_Html* erwartet ein Farbschema, wie es auch in HTML-Dateien zum Einsatz kommt – das Zeichen # gefolgt vom RGB-Wert in hexadezimaler Angabe. *Zend_Pdf_Color_Rgb* legt RGB-Werte als Floats im Wertebereich von 0 bis 1 fest, Graustufen unterstützen die Methoden *Zend_Pdf_Color_Greyscale*, das CMYK-Schema *Zend_Pdf_Color_Cmyk*.

Grafiken einbinden

Bilder (JPG, PNG, TIFF) lassen sich aus Dateien laden, primitive Grafiken auch mit dem Framework selbst zeichnen. Die Klasse *Zend_Pdf_Page* enthält Methoden für Kreise, Ellipsen, Polygone, Rechtecke und Linien oder Teile davon. Um etwa nur ein Kreissegment zu zeichnen, kann man der Methode *drawCircle* zusätzlich Start- und Endwinkel übergeben. Für die Primitive sind optional die Darstellungsmodi wie Füllung und Umrandung einstellbar (Listing 2).

Beim Laden eines Bildes ermittelt die statische Methode *imageWithPath* der Klasse *Zend_Pdf_Image* automatisch den Typ des Bildes. Danach kann man das Bild samt Koordinaten an die *drawImage*-Methode von *Zend_Pdf_Pag* übergeben:

```
<?php
// Bild aus Datei laden
$image = Zend_Pdf_Image::imageWithPath('/tmp/ ⁊
                                    testbild.jpg');
// Bild in Orginalgröße zeichnen
$x1 = 100;
$y1 = 300;
$x2 = $x1 + $image->getPixelWidth();
$y2 = $y1 + $image->getPixelHeight()¬ ;
$page->drawImage($image, $x1, $y1, $x2, $x2);
?>
```

Das Bild lässt sich beim Zeichnen gleich skalieren, wenn für die Koordinaten *$x2* und *$y2* nicht die genaue Höhe und Breite berücksichtigt werden, sondern entsprechend transformierte Werte.

Fazit

Das Zend-Framework erlaubt es, ohne größere Verrenkungen PDF-Dokumente zu generieren und zu ändern. Zwar lassen sich nicht alle Features des PDF-Standards nutzen (Formulare, Signaturen et cetera), dennoch dürften sich die meisten Anwendungsfälle lösen lassen. Es bleibt aber zu hoffen, dass die Implementierung der PDF-API vollständiger und aktueller wird. Trotzdem arbeitet die API performant und ist in ihren Methoden leicht verständlich. Das Jonglieren mit Pixeln und Koordinaten erweist sich zwar manchmal als etwas lästig, aber das liegt weniger an der API als an PDF selbst. (JS)

MARKUS BACH

beschäftigt sich seit 1999 mit PHP. Sein Aufgabenschwerpunkt liegt momentan in der Java-Entwicklung, außerdem ist er als Softwarearchitekt tätig.

Literatur

[1] Rolf Assfalg; PDF; Auf Wunsch Druck; Professionelle Druckausgaben für Internet-Anwendungen; *iX* 1/2004, S. 126

iX-Link0805134

Onlinequellen

[a] Framework-Homepage	framework.zend.com
[b] API des Framework	framework.zend.com/apidoc/core/
[c] PHP-Konfigurationseinstellungen ändern	www.php.net/manual/de/configuration.changes.php
[d] Beispielprogramm	ftp.heise.de/pub/ix/ix_listings



Grails 1.0: Klare Struktur und solide Techniken

Ritterschlag

Dierk König

Nach knapp dreijähriger Entwicklungszeit ist die Version 1.0 von Grails, dem Web-Framework für Groovy und Java, fertig. Einige Neuerungen wie die vereinfachte Umsetzung von REST durch Content Negotiation und Codecs für transparentes Marshalling von JSON- und XML-Parametern bringen Softwareentwicklern noch mehr Komfort.

Für viele Organisationen ist Grails mittlerweile das Werkzeug der Wahl, wenn es um das Erstellen schlanker Webapplikationen auf der Java-Plattform geht. Die Gründe dafür sind so zahlreich wie die Anwender, aber zu einem großen Teil sind es die vier Entwurfsprinzipien des Framework, die diese Auswahl begründen:
– Einfachheit
– Plattform-Integration
– Java-Perspektive
– Reichhaltigkeit

Grails ist einfach zu installieren und bringt alles mit, was man für die Entwicklung benötigt, inklusive Datenbank und Webserver. Voraussetzung ist lediglich ein installiertes JDK.

Konventionen wie die Aufteilung in Domänenmodell, Controller, Views, Jobs und Services mit den zugehörigen Verzeichnissen geben eine Struktur vor, die Grails automatisch anlegt und konsistent befüllt. Ein Entwicklerteam muss sein Build-System nicht mehr konfigurieren oder gar selbst bauen, sondern kann einfache Befehle nutzen wie

```
grails create-app myapp
grails run-app
grails war
```

Um Duplikationen zu vermeiden, kann man Elemente auslagern, Controller-Teile etwa in Filter oder View-Teile in Layouts, Taglibs und Templates. Der Kunstgriff besteht darin, beim Auflösen von Duplikation möglichst wenig neue Komplexität einzuführen, wie sie durch Abhängigkeitsstrukturen oder Konfigurationen entstehen kann. Auch hier helfen einfache Konventionen, wie bei Templates, die nur in Views Verwendung finden, die im gleichen oder einem Unterverzeichnis liegen.

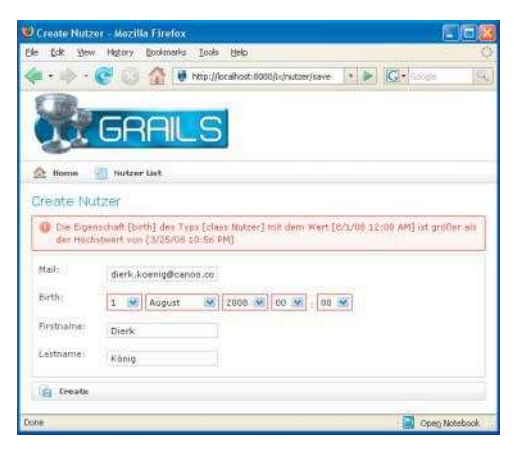
Grails setzt auf der Java Enterprise Plattform auf und integriert die dort etablierten Standards: JavaEE als architektonische Basis, Spring für Applikationsstrukturierung mittels Dependency Injection, MVC und Webflow sowie Hibernate für das objektrelationale Mapping. Die Version 1.0 führt eine domänenspezifische Sprache für ein objektrelationales Mapping ein, sodass Entwickler hierfür nicht mehr zwangsläufig auf Hibernate zurückgreifen müssen.

Neue Projekte sind meist in eine Landschaft zu integrieren, in der schon Frameworks, Bibliotheken oder Komponenten vorhanden sind. Und selbst wenn das nicht der Fall sein sollte, möchte man von der Vielfalt der Java-Open-Source-Projekte profitieren. Grails garantiert dem Anwender diese Flexibilität durch seine nahtlose Integration in die Java-Plattform und die konsequente Einhaltung der Java-Perspektive.

Oft hat ein Entwickler schon Code vorliegen oder möchte einzelne Teile der Applikation lieber in Java schreiben. Grails unterstützt eine beliebige Mischung aus Java und Groovy, wenn auch die Groovy-Variante mehr Komfort bietet. Für Java-Programme muss man die Spring-Konfiguration oder die Hibernate-Mappings wieder selbst vornehmen. Zumindest kann man so aber ein bestehendes Java-Domänenmodell

iX-TRACT

- Nach knapp drei Jahren Entwicklungszeit wurde die Version 1.0 des Web-Framework Grails freigegeben.
- Grails verbindet Java-Frameworks wie Spring und Hibernate mit den dynamischen Eigenschaften der Programmiersprache Groovy.
- In die Release 1.0 sind praktische Erweiterungen eingeflossen, die sich aus der produktiven Arbeit der Open Source Community mit früheren Grails-Versionen ergeben haben.



Builder sind deklarativ genug für die Beschreibung von Views und Datenbank-Schemata und gleichzeitig ausführbar für die Validierung (Abb. 1).

Listing 1: grails-app/domain/Nutzer.groovy

```
class Nutzer {
    String firstname, lastname, mail
    Date   birth

    static constraints = {
        mail   email: true
        birth  max:   new Date()
    }
}
```

Listing 2: NutzerRestTest.groovy

```
String url = 'http://localhost:8080/ix/nutzer/showRest'
assert '''<?xml version="1.0" encoding="UTF-8"?><nutzer id="1">
  <birth>1968-04-19 00:00:00.0</birth>
  <firstname>Dierk</firstname>
  <lastname>Koenig</lastname>
  <mail>dierk.koenig@canoo.com</mail>
</nutzer>''' ==
        "$url/1".toURL().text
def list = new XmlParser().parse("$url/100")
assert ['1'] == list.nutzer.@id
```

Listing 3: grails-app/conf/BootStrap.groovy

```
class BootStrap {
     def init = {
         def dierk = new Nutzer(
                 firstname: 'Dierk',
                 lastname:  'Koenig',
                 mail:      'dierk.koenig@canoo.com',
                 birth:     new Date(68,3,19))
         if (!dierk.save()) {
             println dierk.errors
}  }  }
```

inklusive Mapping wiederverwenden, was einen sanften Migrationspfad für die Ablösung durch Grails eröffnet.

Mit der Release 1.0 wird Grails zu einer Plattform, die nicht nur Bausteine zur Verfügung stellt, sondern Strukturvorgaben macht, den Entwicklungsprozess unterstützt und den gesamten Lebenszyklus der Applikation begleitet.

Kernstücke dieser Plattform sind das auf Gant basierende Build-System und das Plug-in-Konzept. Da Grails selbst bis auf einen minimalen Kern vollständig aus seinen eigenen Plug-ins besteht, lassen sich über Plug-ins alle erdenklichen Effekte erzielen: von eigenen Scaffolding-Befehlen wie *grails generate-webtest* – definiert vom Webtest-Plug-in, um funktionale Tests für ein Domänenobjekt zu erzeugen – bis zur Injektion synthetischer Methoden.

Trotz dieser Mächtigkeit sind Plug-ins denkbar einfach. Sie sind im Grunde übliche Grails-Applikationen plus etwas Zusatzinformation für die Versionierung und das Dependency-Management. Für die Erstellung und das Arbeiten mit Plug-ins stellt Grails folgende Befehle bereit:

```
grails create-plugin
grails package-plugin
grails release-plugin
grails install-plugin
```

Von der Grails-Homepage aus finden Interessierte viele Plug-ins, vom Testing über Security und Suchmaschinen bis zu populären Präsentationstechniken.

Plug-ins eignen sich aber nicht nur dazu, das Funktionsspektrum von Grails zu erweitern. Man kann sie auch zur Strukturierung der eigenen Anwendung nutzen. Jeder Aspekt lässt sich in ein Plug-in auslagern und kann für sich genommen entwickelt und getestet werden. Das Dependency Management sorgt für den Zusammenzug der benötigten Plug-ins. Das ist eines der zentralen Konzepte, die aus Grails eine Plattform machen.

Eine Stärke von Groovy sind Builder, von denen Grails ausgiebigen Gebrauch macht: bei der Definition von Spring Beans, der Beschreibung von Web Flows, für die Anpassung des OR-Mappings, bei der Definition von Constraints auf Domänen-Objekten, der Formulierung von Hibernate Criteria, der Zuordnung von URLs auf Controller und Actions, der Reaktion auf die Anfrage unterschiedlicher Datenformate (Content Negotiation), der Erzeugung strukturierter Formate wie HTML oder JSON, bei der Beschreibung der Build-Aktionen, der Spezifikation funktionaler Tests und generell bei allem, was entfernt wie eine Konfiguration aussieht.

Anders als Dateien in externen Formaten wie XML, die keine Möglichkeit bieten, Logik und Referenzen sauber abzubilden, sind Builder Sourcecode mit der vollen Mächtigkeit der Programmiersprache und haben trotzdem ein deklaratives Erscheinungsbild.

Eine Domänenklasse *Nutzer* soll das illustrieren. Sie definiert Bedingungen für das Format der Mailadresse und eines Geburtsdatums, das nicht in der Zukunft liegen darf (Listing 1).

Ein *ConstraintsBuilder* evaluiert die *constraints*-Closure, wobei die Kombination von deklarativem Charakter und ausführbarer Logik deutlich wird. Die Constraints lesen sich wie eine Konfiguration, sind aber ausführbarer Code, was die Ausdrücke *true* und *new Date()* verdeutlichen. Gleichzeitig liefert der Builder strukturelle Information, die an drei Stellen Verwendung findet: bei der Erstellung der Views für die *create*- und *edit*-Aktionen, für die Validierung des *Nutzer*-Objekts vor der Speicherung und für die Definition des Datenbankschemas.

Konfigurieren über ausführbaren Code

Abbildung 1 zeigt den Versuch, einen *Nutzer* mit Geburtsdatum in der Zukunft anzulegen. Zu beachten ist, welche Strukturinformationen der View aus dem *ConstraintsBuilder* bezieht: nicht nur die Tatsache der Verletzung selbst, die eine Ausführung der Constraints erfordert, sondern auch die Lokalisierung der betroffenen Eigenschaft und die Art der Verletzung – sogar noch mit internationalisierter Fehlermeldung. Der View berücksichtigt außerdem, dass der *mail*-Constraint vor *birth* definiert ist und ordnet danach die Reihenfolge der Eingabefelder an. Properties ohne Constraints folgen am Ende.

Um alle Views und Controller für diese kleine *Nutzer*-Klasse zur Laufzeit zur Verfügung zu haben, genügt die Klasse *grails-app/controllers/NutzerController.groovy*:

```
class NutzerController {
   static scaffold = Nutzer
}
```

Dieses dynamisches Scaffolding genannte Verfahren erzeugt keine Dateien im File-System, sondern weist Grails lediglich an, wie es sich zur Laufzeit verhalten soll. Das ist gerade zu Beginn eines Projekts nützlich, wenn sich das Domänenmodell noch häufig ändert.

Der *NutzerController* soll als Ausgangspunkt für die Anwendung einiger Neuerungen in Grails 1.0 dienen, die sich schön bei der „RESTifizierung“ der Applikation zeigen lassen: Codecs für das Rendering und Binding unterschiedlicher Formate wie XML oder JSON, Content Negotiation und Filter. (Ein lauffähiges Beispiel ist über den *iX*-Listingsserver erhältlich.)

Alle Operationen zum Anschauen, Anlegen, Verändern und Löschen eines Nutzers sollen nicht nur per HTML, sondern auch über eine REST-API möglich sein. Dazu soll zunächst ein einfacher *GET*-Request einen *Nutzer* im XML-Format zurückgeben. Ein Groovy-Script dient als *TestCase* und REST-Client (Listing 2).

Der Test spezifiziert erstens den XML-Text, den die Anwendung bei der Anfrage einer vorhandenen *id* (*1*) liefern soll. Das geschieht mehr der Illustration wegen, denn man darf sich nicht auf die Reihenfolge der Elemente verlassen. Deshalb zeigt die zweite Zusicherung die Anfrage auf eine nicht vorhandene *id* (*100*). Als Ergebnis wird eine Liste aller vorhandenen Nutzer erwartet. Hier stellt der Client mit den Mitteln von Groovy alle *id*-Attribute von allen Nutzer-Elementen in der Resultatliste zusammen.

Damit ein solcher Benutzer beim Starten der Applikation verfügbar ist, befüllt eine Klasse beim *bootstrapping* die Datenbank entsprechend (Listing 3).

REST-Client bewährt sich im Test

Die im *TestCase* verwendete URL legt nahe, dass es im *NutzerController* eine neue Action *showRest* geben soll, die als Parameter die *id* des anzuzeigenden *Nutzer*s übergibt. Zu diesem Zweck bekommt der *NutzerController* eine neue Action (Listing 4).

Anhand seiner *id* holt die dynamische Methode *get* den *Nutzer* von Hibernate. Wird die *id* als Parameter übergeben, verwendet die *get*-Methode sie, ansonsten setzt der Elvis-Operator das Argument auf *0*. Da es hierfür kein Objekt gibt, erzeugt die Methode in dem Fall ein leeres Ergebnis. Das auf diese Weise erhaltene Resultat verwendet die Action weiter. Im Fall einer leeren Ergebnisliste holt *list()* die Liste sämtlicher *Nutzer*. Unabhängig davon, was im Resultat steht, erfolgt die Ausgabe *as XML*, also über den XMLCodec. Für die Operationen zum Anlegen, Verändern und Löschen muss man aus dem übergebenen XML allerdings ein Domänenobjekt machen:

```
def update = {
def nutzer = new Nutzer(params.nutzer) ... }
```

Hier wird erwartet, dass im Eingabestrom des *PUT*-Request der Nutzer im gleichen XML-Format spezifiziert ist wie beim *GET* im *TestCase*. Das Binding von XML auf Domänenobjekte basiert auf Spring Bean Binding und funktioniert nicht nur für REST-Calls, sondern auch für HTML Form Submission. Damit der REST-Client die passende Action findet, kann er direkt einen *PUT*-Request an *nutzer/update* schicken. Es geht aber noch einfacher: per Filter. Jede Grails-Applikation hat eine Datei *UrlMappings*, in der man Requests anhand ihrer Eigenschaften auf Controller oder Views umleiten kann (Listing 5).

Der Client muss seinen Request also nur noch an die *"nutzer"*-URL schicken und wird an die passende Action weitergeleitet. Dies macht den Client robuster gegen serverseitige Änderungen.

Für den Fall, dass ein HTML-Client einen Link auf die *"nutzer"*-URL setzt und die Darstellung nicht in XML, sondern in HTML erfolgen soll, gibt es die Content Negotiation. Dafür erweitert ein *withFormat* die *showRest*-Action, und weil es so einfach ist, wird gleich noch die Ausgabe als JSON erlaubt, um auch den Ajax-Zugriff mit abzubilden.

Die Aufzählungen der unterstützten Formate kann man nachlesen in *grails-app/conf/Config.groovy* unter den *grails.mime.types*, die man selbst erweitern kann. Die Ermittlung der Ausgabeformate lässt sich auf drei Arten „aushandeln":
– über den Accept Header des Request unter Berücksichtigung von Alternativen und ihres Qualitätsfaktors „q" (siehe www.w3.org/Protocols/rfc2616/rfc2616-sec14.html)
– über eine Dateiendung wie in *showRest/1.xml*
– über den *format*-Parameter wie in *showRest/1?format=json*
Ohne spezielle Angabe gilt HTM.

Bleibt noch zu erwähnen, dass XML-Rendering und Binding nicht nur mit einfachen Objekten, sondern auch mit Objektgraphen funktionieren. Generell sieht man nur einen kleinen Ausschnitt, der das Konzept erläutert. Mehr Details enthält die Onlinedokumentation.

Fazit

Grails ist klar in der Architektur, stark in den Konzepten und solide in den verwendeten Techniken. Java-Entwickler bleiben in ihrer gewohnten Welt, was das „Ökosystem" – Laufzeitumgebung, Deployment und Entwicklungswerkzeuge – angeht, und haben gleichzeitig ein neues, leichtgewichtiges „Fahrgefühl".

Die Groovy- und Grails-Community wächst von Tag zu Tag und kann mit der Firma G2one seit Anfang des Jahres genügend Vollzeit-Entwickler für ein nachhaltiges Wachstum vorweisen. Bei Redaktionsschluss galt bereits die Version 1.0.2 als stabil. Auch im Markt häufen sich die guten Nachrichten. SAP hat sein auf Netweaver basierendes Projekt „Composition on Grails" angekündigt. Der führende US-Web-Hoster Contegix stellt sein gesamtes Management auf die Grails-Plattform um. Große Grails-Anwendungen wie *showbiz.sky.com* gehen mit über 180 Millionen Hits im Monat online.

Für die Zukunft kann man eine noch stärkere Nutzung von Grails als technische Plattform auch für Desktop-Anwendungen erwarten. Hier liegt ein Potenzial, das erst ansatzweise genutzt wird. (ka)

Listing 4: Zusatz zu grails-app/controllers/NutzerController.groovy

```
import grails.converters.* // zuoberst einfügen
    def showRest = {
        def result = Nutzer.get(params.id ?: 0)
        result = result ?: Nutzer.list()
        render result as XML
    }
```

Listing 5: Zusatz zu grails-app/conf/UrlMappings.groovy

```
static mappings = {
   "/nutzer/$id?"(controller:"nutzer"){
      action = [GET:"showRest", PUT:"update",
               DELETE:"delete", POST:"save"]
   }
}
```

Listing 6: Content Negotiation

```
    def showRest = {
        def result = Nutzer.get(params.id ?: 0)
        result = result ?: Nutzer.list()
        withFormat {
            html { redirect action:'show'}
            xml  { render result as XML  }
            json { render result as JSON }
        }
    }
```


DIERK KÖNIG

ist Softwareentwickler bei der Canoo Engineering AG in Basel, Committer in den Projekten Groovy und Grails sowie Autor des Buchs „Groovy in Action".

Literatur

[1] Dierk König; Grails-Tutorial I bis III; *iX* 6/07 bis 8/07

Onlineressourcen

Grails-Homepage	grails.org
Groovy-Homepage	groovy.codehaus.org
Grails-Screencasts	grails.org/Grails+Screencasts
Grails-Podcast	grails.org/Grails+Podcast



Samba als primärer Domänencontroller

Metronom

Karolin Seeger

Eine Krönung des Samba-Einsatzes in gemischten Umgebungen ist der Betrieb als primärer Domänencontroller. Vor allem in größeren Umgebungen spielt dabei die Anbindung an einen LDAP-Verzeichnisdienst eine wichtige Rolle.

In den ersten beiden Teilen des Samba-Tutorials stand der Samba-Einsatz als alleinstehender Server und als Mitgliedsserver einer Domäne im Fokus. Dieser Teil erläutert den Einsatz als Domänencontroller, wobei er auch die Anbindung an den Verzeichnisdienst OpenLDAP (LDAP – Lightweight Directory Access Protocol) thematisiert. Die abgedruckten Listings sind teilweise gekürzt. Die vollständigen gibt es über den *iX*-Listing-Service.

In einer Domäne existiert im Gegensatz zu einer Arbeitsgruppe eine zentrale Benutzerdatenbank, der sogenannte SAM (Security Account Manager). Die Anmeldung der Benutzer erfolgt in diesem Konzept nicht lokal an einem Client, sondern zentral an einem der Domänencontroller. Das hat den Vorteil, dass man die Benutzerkonten nicht lokal auf den Clients pflegen muss, sondern dass sie allen Benutzern an allen Domänenmitgliedern zur Verfügung stehen. Jeder Benutzer kann sich also an jedem Client anmelden, sofern dieser Mitglied der Domäne ist.

Von alten und neuen Domänen

Zwischen NT4 und 2000 hat sich das Windows-Domänenkonzept mit Active Directory (AD) maßgeblich geändert. Samba 3 unterstützt derzeit lediglich das NT4-Domänenkonzept, deshalb geht der folgende Text ausschließlich darauf und nicht auf AD ein.

Im NT4-Domänenkonzept existieren in jeder Domäne genau ein primärer (PDC, Primary Domain Controller) und beliebig viele Backup-Domänen-Controller (BDC). Ersterer besitzt einen Schreibzugriff auf die zentrale Benutzerdatenbank. Diese verteilt er auf die BDCs, sie steht dort aber nur als nicht veränderbare Kopie zur Verfügung. Das Hinzufügen oder Entfernen von Benutzern oder Passwortänderungen kann also ausschließlich auf dem PDC erfolgen. Anmeldevorgänge sind aber an BDCs genauso möglich wie an PDCs, damit liegt die Aufgabe von BDCs zum einen in der Ausfallsicherheit und zum anderen in der Lastverteilung bei Anmeldevorgängen.

Samba 3 kann einen NT4 PDC vollständig ersetzen. In diesem Teil des Tutorials geht es darum, einen Samba-PDC aufzusetzen. Es sei trotzdem an dieser Stelle kurz erwähnt, dass Samba auch problemlos als BDC fungieren kann, allerdings benötigt man hierfür einen externen Mechanismus zur Verteilung der Benutzerdatenbank (beispielsweise OpenLDAPs *syncrepl*), da diese Replikation nicht in Samba 3 implementiert ist. Damit Samba sich als PDC für eine Domäne verantwortlich fühlt, sind folgende Parameter erforderlich:

```
[global]
  workgroup = DOM
  security = user
  domain master = yes
  domain logons = yes
```

Die Parameter *workgroup* und *security* waren schon Thema im ersten Teil des Tutorials. Mit *domain master = yes* fungiert der Samba-Server als „Domain Master Browser“ (DMB), pflegt also die Browse-Liste der Domäne. Diese Liste benötigen die Clients für das sogenannte „Browsing“, das Suchen in Microsofts Netzwerkumgebung. Jeder PDC ist Domain Master Browser. Die zentrale Funktion des PDC – das Bereitstellen einer Netzwerkanmeldung – aktiviert der Parameter *domain logons = yes*.

Sobald *domain master = yes* gesetzt ist, registriert der Samba-Server nach einem Neustart des *nmbd* den NetBIOS-Namen „DOM#1b“, das heißt, er ist Domain Master Browser für die Domäne „DOM“. Das lässt sich mit dem Tool *nmblookup* einfach überprüfen, der Aufruf *nmblookup DOM#1b* liefert als Antwort die IP-Adresse des PDC. Mit dem Parameter *domain logons = yes* wiederum registriert Samba den NetBIOS-Namen *DOM#1c*, das heißt, es stellt Logon-Dienste zur Verfügung.

Welche Namen ein Server (oder auch Client) registriert hat, verrät das Kommando *nmblookup -A localhost*, wobei man *localhost* durch einen beliebigen

Rechnernamen ersetzen kann. Listing 1 zeigt ein Beispiel. Der Server dort ist PDC, weil er die Namenstypen *1c* (Logon Server) und *1b* (Domain Master Browser) der Domäne innehat. BANDO ist dabei der Windows-Name des Samba-Servers.

Nun lassen sich schon Clients in die Domäne aufnehmen („joinen“). Voraussetzung hierfür ist, dass der Samba-Benutzer „root“ in der Benutzerdatenbank existiert. Dieser Benutzer ist der Domänenadministrator einer Samba-Domäne und immer berechtigt, Rechner in die Domäne aufzunehmen. Alternativ kann man auch einen normalen Benutzer mit dem Recht ausstatten. Das erfolgt über das Kommando *net rpc rights grant <benutzer> SeMachine AccountPrivilege*.

Damit die Domänenmitglieder auf die Benutzerdatenbank des Domänencontrollers zugreifen dürfen, benötigen sie ein Maschinenkonto in eben dieser Benutzerdatenbank. Beim Beitritt in eine Domäne geschieht nichts anderes, als dass der PDC dieses Konto erzeugt und ein Passwort dafür festlegt. Ein Maschinenkonto ist grundsätzlich ein normales Benutzerkonto, dessen Name aber um ein *“$“* erweitert wird.

Ein Konto kann Samba allerdings nur dann anlegen, wenn auf dem System ein korrespondierendes Unix-Konto existiert. Dieses kann man entweder manuell erzeugen oder Samba in der *smb.conf* ein Kommando zum Anlegen eines Maschinenkontos an die Hand geben. Dazu dient der Parameter *add machine script*. Ein gängiges Beispiel hierfür ist *add machine script = /usr/sbin/useradd -d /nodir -s /bin/false ‚%u’*.

Tritt nun ein Client der Domäne bei, erzeugt Samba das Maschinenkonto Unix-seitig mit obigem Befehl. Das Makro *%u* ersetzt es durch den Namen der Maschine. Das ist deutlich komfortabler, als für jedes Domänenmitglied das Unix-Konto manuell anzulegen.

Benutzerprofile auf dem Server ablegen

Wenn Benutzer nicht ausschließlich an einem Arbeitsplatz tätig sind, sondern häufig die PCs wechseln, können serverbasierte Profile, sogenannte „Roaming Profiles“, sinnvoll sein. Hierbei erfolgt die Speicherung des Windows-Profils nicht lokal auf dem Client, sondern auf dem Samba-Server. Das hat den Vorteil, dass den Benutzern an jeder Arbeitsstation, die Mitglied der Domäne ist, nach der Anmeldung ihre eigene Umgebung (Hintergrundbild, Desktop-Links et cetera) zur Verfügung steht.

Wo die Profile gespeichert werden, bestimmt der Parameter *logon path*. Standardmäßig erfolgt das auf dem Server, genauer gesagt im Verzeichnis *profile*, das sich im Heimatverzeichnis des jeweiligen Benutzers befindet. Da Profile von Windows 2000 und Windows XP nicht kompatibel sind, sollten Anwender, die beide Betriebssysteme einsetzen, diese Standardeinstellung nicht verwenden. Besser ist es, eine dedizierte Freigabe für die serverbasierten Profile zur Verfügung zu stellen, darin pro Benutzer ein Unterverzeichnis anlegen zu lassen und in diesem wiederum pro Windows-Version ein weiteres Unterverzeichnis zu verwenden.

Im globalen Abschnitt der *smb.conf* ist dazu *logon path = \\%N\profiles \%U\%a* zu setzen. *%N* steht für den NetBIOS-Namen des Servers, *profiles* bezeichnet die Profil-Freigabe. *%U* und *%a* sind Makros für den Benutzernamen sowie die Architektur des Betriebssystems des Clients. Die Definition der Freigabe könnte beispielsweise wie folgt aussehen:

```
[profiles]
    path = /data/profiles
    writeable = yes
    profile acls = yes
```

Diese muss natürlich schreibbar sein, damit Samba dort überhaupt Profile speichern kann. Der Parameter *profile acls = yes* sollte in einer Profil-Freigabe immer gesetzt sein, allerdings in keiner anderen Freigabe. Es handelt sich dabei um einen Workaround für das Verhalten von Windows XP im Zusammenhang mit Roaming Profiles. Deshalb sollte man für die Profile auch eine separate Freigabe benutzen. Selbstverständlich kann man die Verzeichnisstruktur in der Profil-Freigabe beliebig anders aufbauen. Wichtig ist allerdings, dass der jeweilige Benutzer in den Verzeichnissen Schreibrechte benötigt.

iX-TRACT

- Samba kann den PDC einer NT4-Domäne vollständig ersetzen.
- Ein Verzeichnisdienst ermöglicht eine zentrale Benutzerverwaltung, die viele Dienste nutzen können.
- Auch Samba lässt sich für die Authentifizierung an einen Verzeichnisdienst anbinden.

Listing 1: *nmblookup -A localhost*

```
bando:~ # nmblookup -A localhost
Looking up status of 127.0.0.1
        BANDO           <00> -         B <ACTIVE>
        BANDO           <03> -         B <ACTIVE>
        BANDO           <20> -         B <ACTIVE>
        DOM             <1b> -         B <ACTIVE>
        DOM             <1c> -         B <ACTIVE>
        DOM             <1e> - <GROUP> B <ACTIVE>
        DOM             <00> - <GROUP> B <ACTIVE>
        MAC Address = 00-00-00-00-00-00
```

Listing 2: Beispiel eines Anmeldeskripts

```
echo Uhrzeit mit dem Samba-Server synchronisieren
net time \\smbsrv1 /set /yes
echo Netzlaufwerke verbinden
net use h: \\smbsrv1\share1
net use i: \\smbsrv1\share2
```

Meldet sich ein Benutzer an einer Domäne an, können die Clients automatisch Skripte ausführen. Oft erfolgt über solche Skripte die Einbindung von Netzlaufwerken oder das Synchronisieren der Systemzeit. Der Administrator kann jedem Benutzer ein eigenes Skript zur Verfügung stellen, aber auch gruppenbasierte Skripte einrichten. Ein typisches Szenario für Letzteres wäre, dass für alle Mitglieder der Gruppe *orga* die gleichnamige Freigabe während des Anmeldevorgangs automatisch als Laufwerk *O:* eingebunden wird.

Voraussetzung für den Einsatz solcher Anmeldeskripte ist eine Freigabe namens *netlogon*. Da es sich um eine Freigabe mit spezieller Funktion handelt, darf der Freigabename nicht variieren.

```
[netlogon]
    path = /var/lib/samba/netlogon
    browseable = no
```

Zusätzlich zu obiger Definition der Freigabe *netlogon*, muss im globalen Abschnitt der *smb.conf* der Parameter *logon script* definiert sein:

```
    logon script = %U.bat
```

Er bestimmt den Namen des auszuführenden Skripts. Die Angabe des *logon script* erfolgt immer relativ zur Netlogon-Freigabe. Listing 2 zeigt, wie ein Anmeldeskript aussehen kann.

Verzeichnisdienst für Samba vorbereiten

In größeren Umgebungen kann es sinnvoll sein, die Systembenutzer in einer LDAP-Datenbank zu verwalten. Hier kann man Benutzer und deren Attribute zentral verwalten und die Datenbank auf andere Server replizieren. Das stellt sicher, dass die Kennungen und Gruppen auf allen Systemen existieren und überall dieselben UIDs/GIDs haben. Diverse Dienste können Benutzerdaten aus LDAP-Verzeichnissen auslesen.

Auch Samba-User lassen sich in LDAP-Datenbanken verwalten. Voraussetzung dafür ist ein laufender LDAP-Server. In diesem Tutorial dient dafür die Open-Source-Implementierung OpenLDAP. Samba arbeitet aber auch mit jedem anderen LDAP-Server zusammen.

Da eine komplette Einführung in OpenLDAP den Rahmen dieses Tutorials sprengen würde, erläutert dieser Artikel nur die wichtigsten Aspekte. Für tiefer gehende Informationen sei auf unser LDAP-Tutorial verwiesen [1-3], Listing 3 zeigt, wie eine ganz einfache OpenLDAP-Konfiguration aussehen kann. Wichtig ist, dass OpenLDAP das Samba-Schema einbindet, dies erledigt die Zeile

```
include   /etc/openldap/schema/samba3.schema
```

Ohne dieses Schema stehen die von Samba benötigten Attribute und Objektklassen wie *sambaSamAccount* nicht zur Verfügung. Außerdem muss man mit *suffix* die Basis des LDAP-Baums beschreiben und via *rootdn* den Administrator der LDAP-Datenbank festlegen:

```
suffix  "dc=samba,dc=org"
rootdn   "cn=Manager,dc=samba,dc=org"
```

Es ist sinnvoll, für Samba einen separaten Benutzer anzulegen, der sich mit dem LDAP-Server verbindet. So lässt sich später über Access Control Lists (ACLs) genau definieren, welche Änderungen Samba vornehmen darf und welche nicht. Der *rootdn* darf stets alle Attribute ändern und ist daher aus Sicherheitsgründen nicht geeignet.

Mit dieser Konfiguration wird der LDAP-Server gestartet. Die LDAP-Datenbank ist jetzt noch leer. Die in der *slapd.conf* angegebene Grundstruktur der Datenbank und Container für Benutzer, Gruppen und Maschinenkonten existieren noch nicht. Für die Grundstruktur und die ersten beiden Benutzer (*samba* und *Manager*) lässt sich die in Listing 4 gezeigte LDIF-Datei (LDAP Data Interchange Format) verwenden. Das Beispiel legt den Benutzer *samba* mit gleichnamigem Passwort an. Dass man Letzteres im realen Einsatz durch ein sicheres Passwort ersetzen sollte, versteht sich von selbst.

Wenn der LDAP-Server läuft, kann der Administrator die Datei mit dem Kommando *ldapadd -f /tmp/samba.ldif -x -W -D „cn=Manager,dc=samba,dc=org“* einlesen. Anschließend befinden sich die in der Datei beschriebenen Objekte in der LDAP-Datenbank. Den Erfolg kann man mit *slapcat* oder einem beliebigen grafischen LDAP-Browser wie Luma oder GQ überprüfen.

Vor dem Samba-Start fehlen noch der Samba-Gastbenutzer *nobody* und ein paar andere Samba-Objekte in der LDAP-DB. Das Kommando *net sam provision* bereitet die LDAP-DB auf Samba vor, indem es die fehlenden Objekte anlegt. Voraussetzung für die Verwendung dieses Kommandos ist ein richtig konfigurierter und laufender Winbind-Daemon.

Listing 3: Einfache LDAP-Konfiguration

```
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/yast.schema
include     /etc/openldap/schema/samba3.schema
pidfile     /var/run/slapd/slapd.pid
argsfile     /var/run/slapd/slapd.args
modulepath     /usr/lib/openldap/modules
access to dn.base=""
     by dn="cn=samba,dc=samba,dc=org" write
     by * read
access to dn.base="cn=Subschema"
     by * read
access to attrs=userPassword,userPKCS12
     by self write
     by * auth
access to attrs=shadowLastChange
     by self write
     by * read
access to *
     by dn="cn=samba,dc=samba,dc=org" write
     by * read
#################################################################
# BDB database definitions
#################################################################
database     bdb
suffix          "dc=samba,dc=org"
checkpoint      1024    5
cachesize       10000
rootdn          "cn=Manager,dc=samba,dc=org"
rootpw          secret
directory     /var/lib/ldap
# Indices to maintain
index     objectClass     eq
index uidNumber               eq
index gidNumber               eq
index memberUid               eq
index   sambaSID              eq
index   sambaPrimaryGroupSID  eq
index   sambaDomainName       eq
index   default               sub
```

Listing 4: Import via *samba.ldif*

```
dn: dc=samba,dc=org
objectClass: top
objectClass: dcObject
objectClass: organization
o: samba.org
dc: samba
dn: cn=Manager,dc=samba,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: Manager
description: LDAP administrator
userPassword: secret
dn: cn=samba,dc=samba,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: samba
description: Samba user to connect to LDAP
userPassword: samba
dn: ou=users,dc=samba,dc=org
objectClass: top
objectClass: organizationalUnit
ou: users
[...]
ou: groups
[...]
ou: idmap
[...]
ou: computers
```

Listing 5: Winbind-Konfiguration

```
workgroup = DOM
idmap domains = DOM
idmap alloc backend = ldap
idmap alloc config:ldap_base_dn =
                              ou=idmap,dc=samba,dc=org
idmap alloc config:ldap_user_dn =
                              cn=samba,dc=samba,dc=org
idmap alloc config:ldap_url = ldap://localhost
idmap alloc config:range = 50000-500000
```

Anpassungen der Winbind-Konfiguration

Früher diente der Winbind, wie im zweiten Teil der Tutorials beschrieben, ausschließlich zum Einsatz auf Mitgliedsservern. Das ist aber inzwischen überholt. Beim Anlegen der Benutzer muss Samba UIDs und GIDs allozieren, und diese Aufgabe kann Winbind übernehmen. Die in Listing 5 beschriebene Konfiguration funktioniert mit Samba-Versionen ab 3.0.25.

idmap domains listet alle Domänen auf, *idmap alloc backend* bestimmt den Speicherort der Zuordnungen von Windows-SIDs zu Unix UIDs/GIDs. In diesem Fall soll das sogenannte Identity Mapping im LDAP erfolgen. Die darauffolgenden *idmap alloc config*-Einstellungen definieren Details zu diesem Backend. *ldap_base_dn* beschreibt, an welcher Stelle des LDAP-Baums Winbind die Zuordnungen speichert. *ldap_user_dn* gibt den Benutzer für die Verbindung zum LDAP-Server an. *ldap_url* nennt die URL des LDAP-Servers und *range* legt den Bereich fest, aus dem UIDs und GIDs stammen können. Für den erfolgreichen Verbindungsaufbau zum LDAP-Server muss man noch das Passwort des *ldap_user_dn* hinterlegen. Dies erfolgt mit dem Aufruf *net idmap secret alloc samba*.

Samba mit dem LDAP-Server verbinden

Damit Samba mit einem LDAP-Server zusammenarbeitet, sind weitere Einstellungen erforderlich. Zunächst muss man das Benutzer-Backend mit *passdb backend = ldapsam* auf LDAP umstellen. Dadurch greift Samba beispielsweise beim Auflisten der Benutzer auf den lokalen LDAP-Server zu.

Damit der Samba-Server nun erfolgreich eine LDAP-Anfrage ausführen kann, muss er sich mit dem LDAP-Dienst verbinden. Dazu benötigt er in der Regel einen Benutzer, da sich anonym nicht alle erforderlichen Daten abfragen lassen. Welchen Samba hierfür

nutzt, legt *ldap admin dn* fest. Am besten ist hierfür eine dedizierte Benutzerkennung. Auf jeden Fall sollte man an dieser Stelle aus Sicherheitsgründen nicht den *rootdn* der LDAP-Konfiguration verwenden.

Ein LDAP-Server speichert Objekte zur Verbesserung der Übersichtlichkeit in unterschiedlichen Containern, den sogenannten „organizational units“ (*ou*). So existiert in der Regel – wie auch in Listing 4 zu sehen – ein Container für Benutzer (beispielsweise *ou=users*), einer für Gruppen (zum Beispiel *ou=groups*) und einer für die Maschinenkonten der Domänenmitglieder (zum Beispiel *ou=computers*). Damit Samba funktionierende LDAP-Suchfilter zusammensetzen und auch Benutzer- oder Maschinenkonten anlegen kann, muss sich der Aufbau der LDAP-Datenbank zumindest teilweise in der *smb.conf* widerspiegeln. Dazu dienen einige Parameter: *ldap suffix* benennt die Basis des LDAP-Verzeichnisses und entspricht *suffix* in der LDAP-Konfigurationsdatei *slapd.conf*. *ldap user suffix* bezeichnet den Container für die Benutzer (relativ zum *ldap suffix*), *ldap group suffix* ist das Pendant für die Gruppen (relativ zum *ldap suffix*) und *ldap machine suffix* das für die Maschinenkonten (relativ zum *ldap suffix*). *ldap idmap suffix* schließlich gibt den Container für die Zuordnungen von Windows SIDs zu Unix UIDs/GIDs (relativ zum *ldap suffix*) an.

Mit *ldapsam:editposix* kann Samba im LDAP-Verzeichnis selber Konten anlegen. Damit erübrigt sich die Verwendung zusätzlicher Skripte wie *smbldap-tools* oder *ldapsmb*. Das ist ein großer Vorteil, da die Konfiguration solcher Skripte durchaus ihre Tücken haben kann. Voraussetzung für die Verwendung von *ldapsam:editposix* ist, dass *ldapsam:trusted* ebenfalls aktiv ist. Ein komplettes Beispiel der LDAP betreffenden Konfigurationsparameter findet sich in Listing 6.

Wie oben erwähnt, verwendet Samba den via *ldap admin dn* definierten Benutzernamen, um sich mit dem LDAP-Server zu verbinden. Für diesen muss man noch per *smbpasswd -W* das zugehörige Passwort hinterlegen. Jetzt lässt sich die LDAP-DB mit dem Aufruf *net sam provision* um die für Samba notwendigen Objekte erweitern (siehe Listing 7). Anschließend starten auch *smbd* und *nmbd* erfolgreich.

Mit *pdbedit -L* kann man sich nun testhalber die Liste der Samba-Benutzer anzeigen lassen. Klappt der Verbindungsaufbau mit dem LDAP-Server, liefert der Aufruf eine Liste aller Benutzer. Falls nicht, muss man auf Fehlersuche gehen. Der erste Schritt sollte verifizieren, ob der LDAP-Server überhaupt läuft und ob ein Verbindungsaufbau als *ldap admin dn* funktioniert. Dazu kann beispielsweise folgender Befehl dienen:

```
ldapsearch -x -D "cn=samba,dc=samba,dc=↵
    org" -W -b "dc=samba,dc=org" objectClass=*
```

Eine beispielhafte Samba-Konfiguration mit LDAP-Anbindung stellt Listing 8 dar. Serverbasierte Profile, Home-Laufwerke und Anmeldeskripte fehlen hier zur Verbesserung der Übersichtlichkeit.

Modifikationen am Betriebssystem

Schon der erste Teil des Tutorials erläuterte, dass Samba-Benutzer immer ein gleichnamiges Unix-Konto als Pendant haben müssen, damit eine UID vorhanden ist und der Kernel die Zugriffskontrolle durchführen kann. Der große Vorteil des Winbind in solch einem Setup liegt darin, dass er Benutzer- und Maschinenkonten zur Verfügung stellen kann. Im Endeffekt sorgt er dafür, dass Samba die Konten in der LDAP-Datenbank anlegt.

Diese Benutzer muss aber auch das Betriebssystem kennen, um beispielsweise auf Dateisystemebene Zugriffsrechte überprüfen zu können. Dazu muss der Administrator den „Name Service Switch“-Mechanismus so konfigurieren, dass das System sowohl Winbind als auch LDAP nach Benutzern und Gruppen fragt. Dazu muss er in */etc/nsswitch.conf* die *passwd-* und *group*-Anweisungen um die Einträge *ldap* und *winbind* erweitern:

```
passwd: compat ldap winbind
group:  compat ldap winbind
```

Voraussetzung hierfür ist, das die Bibliotheken *libnss_winbind.so* (im Samba-Winbind-Paket enthalten) und *libnss_ldap.so.2* (extra LDAP-Paket, beispielsweise *nss_ldap*) auf dem System vorliegen.

Tutorialinhalt

Teil I: Stand-alone-Samba-Server

Teil II: Mitgliedsserver in einer Windows-Domäne

Teil III: Ein Samba-Server als PDC

Listing 6: LDAP-Anpassungen der *smb.conf*

```
passdb backend = ldapsam
ldap admin dn = cn=samba,dc=samba,dc=org
ldap suffix = dc=samba,dc=org
ldap user suffix = ou=users
ldap group suffix = ou=groups
ldap machine suffix = ou=computers
ldap idmap suffix = ou=idmaps
ldapsam:trusted = yes
ldapsam:editposix = yes
```

Listing 7: LDAP-Datenbank bevölkern

```
bando:~ # net sam provision
Checking for Domain Users group.
Adding the Domain Users group.
Checking for Domain Admins group.
Adding the Domain Admins group.
Check for Administrator account.
Adding the Administrator user.
Checking for Guest user.
Adding the Guest user.
Checking Guest's group.
Adding the Domain Guests group.
```

Listing 8: Samba-Konfiguration mit LDAP

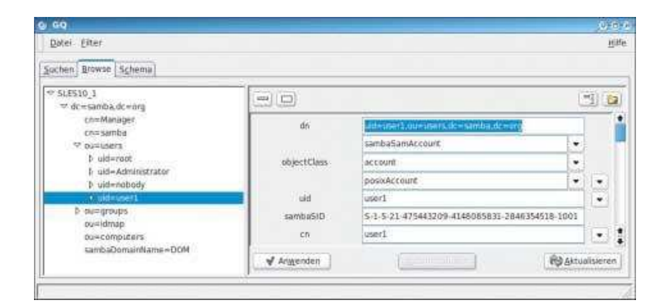
```
[global]
     # Samba als PDC
     workgroup = DOM
     security = user
     domain logons = yes
     domain master = yes
     # WINS-Server
     wins support = yes
     # Informationen fuer LDAP-Zugriffe
     passdb backend = ldapsam
     ldap admin dn = cn=samba,dc=samba,dc=org
     ldap suffix = dc=samba,dc=org
     ldap user suffix = ou=users
     ldap group suffix = ou=groups
     ldap machine suffix = ou=computers
     ldap idmap suffix = ou=idmaps
     ldapsam:trusted = yes
     ldapsam:editposix = yes
     # Winbindd-Konfiguration
     idmap domains = DOM
     idmap alloc backend = ldap
     idmap alloc config:ldap_base_dn = ou=idmap,dc=samba,dc=org
     idmap alloc config:ldap_user_dn = cn=samba,dc=samba,dc=org
     idmap alloc config:ldap_url = ldap://localhost
     idmap alloc config:range = 50000-500000
```

Listing 9: */etc/ldap.conf*

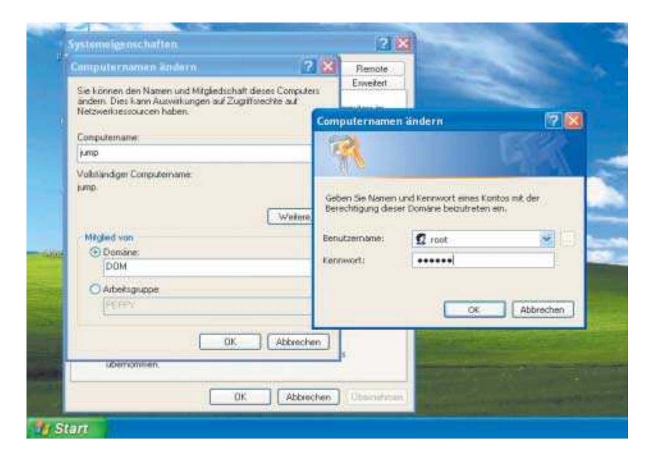
```
host 127.0.0.1
base dc=samba,dc=org
ldap_version 3
bind_policy soft
binddn cn=Manager,dc=samba,dc=org
bindpw secret
rootbinddn cn=Manager,dc=samba,dc=org
port 389
#ssl start_tls
scope sub
pam_password crypt
nss_base_passwd         dc=samba,dc=org?sub
nss_base_group          ou=groups,dc=samba,dc=org?one
```

Listing 10: *root.ldif*

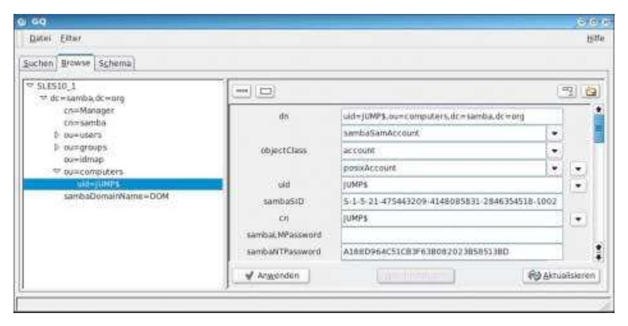
```
dn: cn=root,ou=groups,dc=samba,dc=org
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: root
gidNumber: 0
sambaSID: S-1-5-21-634692503-4291501469-4281879028-1008
sambaGroupType: 2
displayName: Unix Group root
description: Unix Group root
dn: uid=root,ou=users,dc=samba,dc=org
objectClass: account
objectClass: posixAccount
objectClass: sambaSamAccount
uid: root
cn: root
uidNumber: 0
homeDirectory: /root
sambaSID: S-1-5-21-634692503-4291501469-4281879028-1000
displayName: root
sambaPasswordHistory:
00000000000000000000000000000000000000000000000000000000
sambaAcctFlags: [U          ]
gidNumber: 0
```



Via GQ lässt sich schnell überprüfen, ob das Anlegen des Testbenutzers funktioniert hat (Abb. 1).



Für den Domänenbeitritt dient nicht die Administrator-Kennung, sondern der Benutzer *root* (Abb. 2).



Nach dem Domänenbeitritt eines Rechners taucht das Maschinenkonto automatisch im LDAP-Baum auf (Abb. 3).

Damit nun das Linux-System den LDAP-Server abfragen kann, sind auch hier noch einige Dinge zu konfigurieren. Das geschieht in der LDAP-Client-Konfigurationsdatei */etc/ldap.conf* (siehe Listing 9).

Anlegen eines Benutzers als Test

Hierbei kommt es vor allem auf folgende Einstellungen an, das vollständige Beispiel gibt es über den *iX*-Listingservice: *host* nennt Hostname/IP-Adresse des zu befragenden LDAP-Servers und *base* die Basis des LDAP-Baums (siehe *slapd.conf*). *binddn* gibt den Benutzer zum Verbinden mit dem LDAP-Server an und *bindpw* das dazugehörige Passwort. *nss_base_passwd* bezeichnet den Container für die Benutzer und *nss_base_group* den mit den Gruppen. *ssl start_tls* sorgt für eine verschlüsselte Verbindung. In dieser einfachen Beispielkonfiguration ohne Verschlüsselung muss man diese Einstellung deaktivieren.

Nun sollte auch *getent passwd* die Unix-Benutzer aus dem LDAP-Verzeichnis auflisten. Zu Testzwecken kann man einen Beispielbenutzer anlegen.

Vor dem Ausprobieren, ob das Anlegen neuer Benutzer funktioniert, muss man den Benutzer *root* im LDAP-Baum anlegen. Da dieser als primäre Gruppe der Gruppe *root* mit der GID 0 zugeordnet ist, ist auch diese Gruppe anzulegen. Listing 10 zeigt eine passende LDIF-Datei. Dabei muss man darauf achten, das Attribut *sambaSID* für beide Objekte vor der Anwendung an den korrekten Domänen-SID anzupassen. Anschließend fügt der Aufruf

```
ldapadd -x -D "cn=Manager,dc=samba,dc=↵
org" -f /tmp/root.ldif -W
```

die Objekte in den LDAP-Baum ein. Ein nachfolgendes *smbpasswd root* setzt das Samba-Passwort für den Benutzer *root*.

Nun lässt sich per *net rpc user add user1 -U root* testen, ob Samba tatsächlich Unix- und Samba-Konten anlegen kann. Nach der Passwortabfrage sollte das Kommando *Added user user1* zurückliefern. Mit einem LDAP-Browser wie GQ lässt sich das Ergebnis überprüfen, Abbildung 1 zeigt den neu angelegten Benutzer.

Ein weiterer Test ist das Hinzufügen eines Rechners in die Domäne. Auch das sollte jetzt problemlos funktionieren (siehe Abb. 2). Wie in Abbildung 3 zu sehen, taucht das Maschinenkonto nach dem erfolgreichen Beitritt der Domäne in der LDAP-DB auf.

Fazit

Obwohl immer mehr Hilfsmittel wie *net sam provision* und *ldapsam:editposix* Administratoren das Leben inzwischen etwas erleichtern, ist gerade das Verbinden von Samba mit LDAP kein einfaches Unterfangen. Es gibt viele Hürden und Stolpersteine.

Im Laufe dieses Tutorials sollte deutlich geworden sein, dass Samba sehr viele Aufgaben bewältigen kann und sich gewisse Grundfunktionen wirklich einfach und schnell in Betrieb nehmen lassen. Wer an dieser Stelle ins Zweifeln kommt, kann gerne mal einen Windows NT4-PDC und einen Samba-PDC parallel aufsetzen … ;-)

Es gibt allerdings auch komplexere Setups und dazu zählt sicherlich die Anbindung an einen Verzeichnisdienst. (avr)

KAROLIN SEEGER

ist als Samba-Release-Managerin Mitglied im Samba-Team und bei der Göttinger SerNet GmbH in diesem Bereich als Consultant und Dozentin tätig.

Literatur

[1] Daniel Amthor, Thilo Rößler; Verzeichnisdienst; Einmal muss reichen; LDAP-Tutorial I: Installation und Aufbau der Hierarchie; *iX* 6/2006, S. 136

[2] Daniel Amthor, Thilo Rößler; Verzeichnisdienst; Bei der Meldebehörde; LDAP-Tutorial II: Suche, DIT-Aufteilung, Authentifizierung; *iX* 7/2006, S. 158

[3] Daniel Amthor, Thilo Rößler; Verzeichnisdienst; Einmal genügt; LDAP-Tutorial III: Replikation, Authentifizierung, Sicherheit; *iX* 8/2006, S. 151

Automatische Makefile-Rebuilds verhindern

Ausgetrickst

Michael Riepe

Gnu-Tools wie *automake* erleichtern Entwicklern die Arbeit erheblich. Auf der Anwenderseite verursachen sie jedoch gelegentlich Schwierigkeiten – die man mit ein paar Tricks umgehen kann.

Trotz zahlreicher Alternativen verwenden viele Entwickler von Open-Source-Software immer noch *make*, um ihre Programme zu übersetzen. Allerdings schreiben sie die Makefiles immer seltener selbst. Stattdessen setzen sie meist die Gnu-Tools *automake* und *autoconf* ein.

Während *automake* dem Entwickler die Arbeit enorm erleichtert, hält es für den Anwender einige Tücken bereit. So enthält ein von *automake* generiertes Makefile nicht nur die Übersetzungsregeln, sondern auch Anweisungen, wie das Makefile selbst neu zu generieren ist. Die schlagen immer dann zu, wenn die Zeitstempel der betroffenen Dateien durcheinandergeraten – etwa beim Kopieren der Dateien oder beim Einspielen von Patches. Aber auch, wenn das Arbeitsverzeichnis per NFS gemountet ist und die Uhren von Client und Server nicht synchron laufen.

Lästige Automatik

Hat man die passenden Werkzeuge installiert, generiert *make* in so einem Fall zuerst die gesamte Übersetzungs-Infrastruktur neu: Aus jedem *Makefile.am* entsteht ein *Makefile.in*, aus *configure.in* oder *configure.ac* sowie dem ebenfalls automatisch erzeugten *aclocal.m4* baut *autoconf* ein neues *configure* zusammen. Das startet anschließend erneut, um aus jedem modifizierten *Makefile.in* ein neues, aktuelles *Makefile* zu erzeugen.

Dabei kann allerhand schiefgehen – vor allem, wenn der Nutzer andere Versionen von *automake* und *autoconf* installiert hat als der Entwickler. Oft sind die generierten Makefiles unbrauchbar. Auch beschwert sich *autoconf* häufig über undefinierte Makros, weil der Erneuerungsprozess ein unvollständiges *aclocal.m4* erzeugt hat. In dem Fall schlägt generell auch der erneute *configure*-Lauf fehl – die Software lässt sich nicht mehr übersetzen.

Zwar kann man falsche Zeitstempel oft mit dem Befehl *make –t* korrigieren: Statt die gewünschten Dateien neu zu übersetzen, setzt das Kommando einfach ihre *mtime* auf die aktuelle Uhrzeit. Das funktioniert jedoch nicht beim Makefile selbst oder bei den Dateien, aus denen es entsteht, weil *make* darauf besteht, sie zu aktualisieren, bevor es mit der eigentlichen Arbeit beginnt.

Touch-a, touch-a, touch me

Will der Nutzer *automake* ein Schnippchen schlagen, muss er daher selbst Hand anlegen – etwa indem er die Zeitstempel der „veralteten“ Dateien mit dem Programm *touch* neu setzt. Allerdings muss er dabei Vorsicht walten lassen: *touch* legt normalerweise Dateien an, falls sie noch nicht existieren. Bei der Gnu-Version kann man dem mit der Option *–c* entgegenwirken.

Eine Liste der zu „berührenden“ Dateien kann man mit *find* zusammenstellen. Es empfiehlt sich jedoch, nicht nach den Zieldateien – etwa *Makefile.in* – zu suchen, sondern nach den Ursprungsdateien, aus denen sie entstehen. Anschließend kann man mit *sed* die Namen ändern (siehe Listing 1).

Neben Makefiles kann *configure* auch Header-Dateien mit Definitionen erzeugen, die sich direkt in C/C++-Code einbinden lassen. Gewöhnlich hören sie auf den Namen *config.h*. Das Programm *autoheader* erzeugt dazu ein passendes Template, in der Regel *config.h.in*. Der Entwickler kann jedoch in *configure.in* beziehungsweise *configure.ac* beliebige Namen vorgeben. Die Zeile *AC_CONFIG_HEADER(defs.h)* etwa veranlasst *autoheader*, eine Datei *defs.h.in* zu erstellen, aus der später *defs.h* entsteht. Soll die Template-Datei zum Beispiel *defs.in* heißen, kann man ihren Namen mit einem Doppelpunkt getrennt anhängen: *defs.h:defs.in*.

Da *configure.in* und *configure.ac* für den Unix-Makroprozessor *m4* geschrieben sind, bietet es sich an, auch die Namen der Templates mit einem *m4*-Skript zu extrahieren (siehe Listing 2). Der Befehl *sinclude* bindet eine andere Datei ein, sofern sie existiert. Mit *divert* lässt sich die Ausgabe dirigieren: *divert(0)* schickt den folgenden Text zur Standardausgabe, *divert(-1)* ins digitale Nirvana. *dnl* leitet einen einzeiligen Kommentar ein. In der Ausgabe des Skripts erscheinen daher nur die Argumente der vorher definierten Makros.

Die *for*-Schleife in der Shell-Funktion *findfiles* bereitet die gelieferten Namen auf. Damit der Aufruf von *m4* funktioniert, müssen die Skripte im selben Verzeichnis liegen und – bis auf die zusätzliche Endung *.m4* – denselben Namen besitzen. Beim Autor leisten die beiden als *autofool* und *autofool.m4* seit Jahren gute Dienste. (mr)

Listing 1

```
findfiles() {
     find . -name aclocal.m4 -print
     find . -name configure.in -print | sed 's,\.in$,,'
     find . -name configure.ac -print | sed 's,\.ac$,,'
     find . -name Makefile.am -print | sed 's,\.am$,.in,'
     for f in $(m4 $0.m4); do
          case $f in
               (*:*) echo ${f#*:};;
               (*) echo $f.in;;
          esac
     done
}
touch -c $(findfiles)
```

Ein einfaches Shell-Skript setzt die Zeitstempel der gewünschten Dateien neu.

Listing 2

```
divert(-1)
define(`AC_CONFIG_HEADERS', `divert(0)'$1
`divert(-1)')dnl
define(`AC_CONFIG_HEADER', `divert(0)'$1
`divert(-1)')dnl
define(`AM_CONFIG_HEADER', `divert(0)'$1
`divert(-1)')dnl
changequote([, ])
sinclude(configure.in)
sinclude(configure.ac)
divert(0)dnl
```

Die zusätzlich benötigten Dateinamen lassen sich mit wenigen Zeilen *m4*-Code extrahieren.

Universal Serial Bus mal anders

Fröhliche Busfahrten

Kai König

Seit der Einführung von USB gehören frühere PC-Peripherieschnittstellen der Vergangenheit an. Der universelle Bus ist aber nicht nur für Druckerschnittstellen et cetera gut, sondern bringt auch die Puppen zum Tanzen.

Die Spezifikation des Universal Serial Bus haben 1995 Microsoft, Intel, Philips und US Robotics erarbeitet. Ziel war ein neuer und einheitlicher Peripheriebus für PC-Systeme und die langfristige Ablösung von Parallelport, verschiedenen seriellen Schnittstellen, PS/2-Bus sowie externen SCSI-Geräten. Es erscheint rückblickend nicht verwunderlich, dass es weitere drei Jahre und USB 1.1 brauchte, um die Kinderkrankheiten der Plattform auszubügeln. Mit der Version 2.0 schwenkte USB ab 2000 auf Erfolgskurs – nicht zuletzt aufgrund einer deutlichen Verbesserung der Übertragungsbandbreite mit Hi-Speed USB (480 MBit/s).

Heute existieren verschiedene Erweiterungen der USB-Spezifikation, die im Jahr 2008 verwendete Version ist allerdings immer noch die 2.0. Das USB Implementers Forum (www.usb.org/home/) als die für die Spezifikation und Plattformentwicklung verantwortlich zeichnende Industrieorganisation arbeitet zurzeit an USB 3.0 – eine Spezifikation soll noch in diesem Jahr kommen, und erste kommerzielle Produkte sind für 2009 oder 2010 zu erwarten.

Schaut man sich auf dem Markt der erhältlichen USB-Geräte um, findet man zunächst eine Vielzahl sinnvoller und nützlicher Peripheriegeräte wie Tastatur, Maus, Drucker, Scanner oder externe Laufwerke. In die letzte Kategorie fallen die oft locker als „USB-Stick“ oder „Flashdrive“ bezeichneten Speichermedien. Mit der USB-Spezifikation im Hinterkopf handelt es sich dabei um Geräte der Klasse 08h (Mass Storage). Bei dem zurzeit hinsichtlich der Speicherkapazität größten erhältlichen Flashdrive im Format eines USB-Sticks scheint es sich um das 64 GByte fassende USB 2.0 Bus Drive Pro 2 der Firma Buslink zu handeln (www.buslinkbuy.com/products.asp?sku=BDP2%2D64G%2DU2). Der Preis ist ebenfalls ordentlich: Für schlappe 4399,99 US-Dollar kann man das Speichermedium sein Eigen nennen.

Strom aus eigener Quelle

Auf die technischen Details von USB soll dieser Artikel nicht eingehen (interessierte Leser können im Wikipedia-Eintrag zu USB unter en.wikipedia.org/wiki/Universal_Serial_Bus eine Vielzahl weiterführender Informationen zu USB finden). Im Zentrum steht hier vor allem die Tatsache, dass die USB-Schnittstelle eine Stromzufuhr für Peripheriegeräte bereitstellt. Dabei handelt es sich um eine Spannung von 5 Volt und eine maximale Stromstärke von 500 mA. Die Spezifikation sieht auch verschiedene Ausnahmen für USB-Hubs mit oder ohne eigene Stromzufuhr vor, für einzelne Peripheriegeräte kann man jedoch mit den hier angegebenen Werten als Richtschnur gut arbeiten.

Inspiriert durch den im Web-Kuriositätenkabinett der Ausgabe 8/2006 vorgestellten USB-Cooler (www.heise.de/ix/artikel/2006/08/156/) hat sich der Autor auf die Suche nach anderen Absonderlichkeiten im Dschungel der USB-Peripheriegeräte gemacht. Während der letzten Jahre und seit dem Erscheinen von USB 2.0 hat sich ein bislang ungeahnter Markt von USB-Gadgets aller Art entwickelt – man kann fast schon davon ausgehen, dass es zu einem x-beliebigen Spielzeug, Gimmick oder anderen Zeitverschwender auch eine USB-Version gibt – solange die vom USB-Port gelieferten 5 V und 500 mA ausreichend Strom liefern.

Im Zuge der grassierenden Green-IT-Welle ist der Ecobutton (www.eco-button.com) zu betrachten. Dabei handelt es sich um einen Quizbuzzer-ähnlichen USB-Knopf, der als visuelle Erinnerung an die verschiedenen Energiesparmodi eines PCs dienen soll. Drückt der Benutzer ihn, schaltet die dazugehörige Software den PC in einen Energiesparmodus. Der Nutzen ist offensichtlich, wenngleich sich ein identischer Effekt mit der konsequenten Nutzung der systemseitigen Energiesparfunktionen erzielen ließe oder der Bediener den PC einfach nach vollendeter Arbeit abschalten könnte. Menschen sind aber offensichtlich eher dazu bereit das zu tun, wenn sie einen runden Schalter mit einer ebenso runden 2D-Karte der Welt vor sich liegen haben. Eine Version für den Mac ist im Moment noch nicht erhältlich, aber bereits angekündigt.

In Urlaubsorten oder im Vergnügungsviertel der nächsten Großstadt findet man oft Automatenspielhallen oder „Arcades“. Neben Rennsimulatoren und Spielen wie Pacman oder Space Invaders sind Tanzautomaten ein beliebter Spaß. Die USB-Version davon (www.gadgetshop.com/Gadgets/TechnoGadgets/USB_Gadgets/PRDOVR~297242/USB+Dance+Mat.jsp) benötigt eine Grundfläche von nur 100 Quadratzentimetern, und Zeige- sowie Mittelfinger übernehmen die Funktion der Beine. Das Set kommt mit einer kleinen Tänzerinnenpuppe aus Pappe, die man sich für den gepflegten Büro-Fingertanzwettbewerb überstreifen kann.

Ins Büroumfeld passt auch der USB WPM Speedometer, ein Tachometer-ähnliches USB-Gerät, das die Tippgeschwindigkeit eines PC-Bedieners misst (www.ubergizmo.com/15/archives/2008/02/usb_wpm_speedometer.html). Als Extra-Gimmick bietet es einen täglichen Wortzähler und eröffnet somit direkt mehrere Möglichkeiten für spannende Unterhaltung während der Arbeitszeit.

Nachdem die Wettkämpfe dann gelaufen sind, ist zu erwarten, dass verschiedene (unterlegene) Kollegen ihre aufgestauten Spannungen und Aggressionen abbauen müssen. USB-getriebene Raketenwerfer (mit Raketen aus Schaumstoff) sind ja inzwischen bereits

ein alter Hut (www.thinkgeek.com/geektoys/warfare/8a0f/). Neu hingegen ist die Variante mit Webcam und Unterstützung für MSN Instant Messenger (usb.brando.com.hk/prod_detail.php?prod_id=00401). Mit diesen Spielzeugen bekommt auch der tägliche Kampf um den Bürolocher eine neue Qualität.

Zwei weitere Alternativen zum Abbau von Bürofrustration sind der Punch Head und das USB Whack It. Beim Punch Head (www.punch-head.com) handelt es sich um ein generisches Gummigesicht mit USB-Anschluss und einer Software, die am Monitor die Auswirkungen jeglicher Interaktion mit dem Punch Head am Foto des Lieblingsfeindes anzeigt. Die kommerzielle Verfügbarkeit ist für März 2008 angekündigt. Das USB Whack It (www.gizoo.co.uk/Products/PCGaming/PCGagets/USBWhackIt.htm) ist eine Variante des Spiels Whack-a-mole, bei dem man kleine Plastiktiere mit einem Gummihammer schlagen muss, sobald ein Mechanismus sie nach oben schnellen lässt. Anstelle von Maulwürfen bieten verschiedene Versionen nahezu beliebig viel anderes Getier. USB Whack It ist friedlicher und man nutzt nur den Zeigefinder, um kleine Männchen schnell wieder in ihre Halterungen zu drücken.

URLs auf einen Blick

www.usb.org/home/
www.buslinkbuy.com/products.asp?sku=BDP2%2D64G%2DU2
en.wikipedia.org/wiki/Universal_Serial_Bus
www.heise.de/ix/artikel/2006/08/156/
www.eco-button.com
www.gadgetshop.com/Gadgets/TechnoGadgets/USB_Gadgets/PRDOVR~297242/USB+Dance+Mat.jsp
www.ubergizmo.com/15/archives/2008/02/usb_wpm_speedometer.html
www.thinkgeek.com/geektoys/warfare/8a0f/
usb.brando.com.hk/prod_detail.php?prod_id=00401
www.punch-head.com
www.gadgetshop.com/Gadgets/TechnoGadgets/USB_Gadgets/PRDOVR~322644/USB+Putter+Returner.jsp
www.iwantoneofthose.com/usb-chameleon/index.html
www.thinkgeek.com/clearance/megadeals/7825/
www.gizoo.co.uk/Products/PCGaming/PCGadgets/USBWhackIt.htm

Wer weitere URLs zum Thema kennt, hat die Möglichkeit, sie der Online-Version (www.heise.de/ix/artikel/2008/05/146/) hinzuzufügen.

Für friedliche Entspannung sorgt der USB Putter Returner (www.gadgetshop.com/Gadgets/TechnoGadgets/USB_Gadgets/PRDOVR~322644/USB+Putter+Returner.jsp). Als kleines Tischgerät findet es seinen Platz selbst in der kleinsten Schreibtischnische und erlaubt es auch Mitarbeitern ohne Chefbüro, an ihrem Handicap zu arbeiten. Der elektrische Mechanismus des USB Putter Returner sorgt dafür, dass der Ball wieder zum Putter zurückkommt und man nahtlos weiter üben kann. Der Höhepunkt der Entspannung und Sinnlosigkeit ist das USB Chameleon (www.iwantoneofthose.com/usb-chameleon/index.html). Bequem findet es seinen Platz auf dem Monitor oder der Kante des Flachbildschirms, rollt die Augen und streckt gelegentlich die Zunge heraus, um Jagd auf Fliegen zu machen. Leider kann es nicht seine Farbe ändern, aber es ist bestimmt nur eine Frage der Zeit, bis jemand eine Kreuzung aus der USB Lava Lampe (www.thinkgeek.com/clearance/megadeals/7825/) und dem USB Chameleon erfindet. (ka)

Vor 10 Jahren: Reif sein ist nicht alles

Schon 1998 prophezeiten wir, dass ab jetzt mit IP-Telefonie Geld verdient werden könne. Aber nicht immer fängt der frühe Vogel einen Wurm.

Kennen Sie den Film „Die Reifeprüfung“? Kurz zusammengefasst, wird da ein junger Mann von einer reifen Frau vernascht und bricht am Ende gegen ihren Willen mit ihrer Tochter auf zu neuen Ufern. Kein IT-Thema? Von wegen: Man kann diese Handlung auf die technische Entwicklung der IP-Telefonie übertragen: Da war eine junge Technik, die mit einer reiferen Frau in Gestalt der großen TK-Unternehmen wie „Ma Bell“ und „Tante Telekom“ zusammenkommt. Doch erst mit ihren Nachkommen, den agilen Töchtern und ihren DSL-Angeboten, wurde die IP-Telefonie zusammen mit der Multimedia-Flatrate ein großes Thema, dass den Müttern heute schwer zu schaffen macht.

Als *iX* in Ausgabe 5/98 unter dem Titel „Reifeprüfung“ davon berichtete, dass 1998 das Jahr des Geldverdienens mit IP-Telefonietechnik werden sollte, da war die Welt noch in Ordnung. IP-Telefonie in Firmen über ISDN und vor allem das kostengünstige Fax over IP mittels Gateway-Lösungen sollten von der nötigen Reife der Technik künden. Die großen TK-Firmen und die Internet-Provider dachten an einen ordentlich geregelten Markt für professionelle Dienstleistungen. Mit keinem Wort ist im Artikel der Privatkunde bedacht, viel ist dagegen die Rede von der Aufrüstung von Nebenstellenanlagen und die IP-Integration in DV-Netze. Schlappe 1810 DM pro Port wurden damals verlangt und auch gezahlt, ein ISDN-Gateway für 20 000 DM mit 8 möglichen Gesprächsverbindungen wurde als kostengünstige Lösung gepriesen.

Bleibt die Frage, ob 1998 wirklich das Jahr des Geldverdienens mit Voice over IP war. In der Rückschau sieht es nicht danach aus. Nach den Marktzahlen von Pulver Communications kam der Anteil von Voice-over-IP-Gesprächen bis zum Jahr 2000 nicht über einstellige Prozentzahlen hinaus. Das änderte sich erst, als sich aus der halbherzigen Integration in Telefonanlagen Anlagen entwickelten, die komplett auf IP-Telefonie setzten, als mit SIP ein Standard für die Vernetzung von Telefonsystemen aufkam und vor allem, als die private Verbreitung von DSL-Anschlüssen das Aufkommen von Diensten wie Skype ermöglichte.

Heute ist die IP-Telefonie ein Standard mit Flatrate-Anschlüssen im Haus, der auch die mobile Kommunikation, erreicht hat. Viele Firmen nutzen bei mobilen Auslandstelefonaten ihrer Mitarbeiter Gateways und IP-Netze, um die Kosten einzudämmen. Windows Vista wurde von Microsoft erst freigegeben, als der „Skype-Kompatibilitätsmodus“ zufriedenstellend funktionierte. Wenn 1998 also das Jahr der Reifeprüfung war, dann war die dramatische Schlussszene dieser Kommunikationsgeschichte noch nicht gedreht. Die Tochter, die der junge Mann im Film direkt vom Traualtar entführen konnte, war schlicht noch nicht auf der Bühne erschienen. *Detlef Borchers* (JS)

MEHR KBYTES

Java

Als Sun Microsystems am 23. Mai 1995 die Programmiersprache Java und den Browser Hotjava vorstellte, begann der Hype nicht gleich. Und die seinerzeit so omnipräsenten Applets, mit denen, wer etwas auf sich hielt, seine Website schmückte, sind fast in der Versenkung verschwunden. Die Sprache ist geblieben. Die Bücher ebenfalls. Und wie nicht anders zu erwarten sind neue hinzugekommen.

Prentice Hall und O’Reilly haben schon in den Neunzigerjahren Serien von Java-Büchern veröffentlicht und teilweise übersetzt. Deutschsprachige Java-Bibeln sind zwar dünn gesät, aber es gibt sie – und das immer in Neuauflagen, wenn die Version wechselt.

Guido Krügers „Java Programmierung“ liegt jetzt in der fünften Auflage vor und deckt die Standard-Edition in der Version 6 ab. Für das Update hat er mit Thomas Stark einen Koautor bekommen, der seinerseits schon ein Werk zur Sprache veröffentlicht hat. Aber der Reihe nach. „Java Programmierung“ wiegt mit seinen 1300+ Seiten schwer in der Hand und eignet sich nicht fürs mobile Arbeiten. Allerdings enthält die DVD das Werk in einer HTML-Fassung. Eine erprobte Einführung in die Sprache, Objektorientierung und GUI-Programmierung (AWT, Swing).

Christian Ullenbooms „Java ist auch eine Insel“ darf momentan die siebte Auflage erleben und behandelt auf mehr als 1400 Seiten dieselbe Java-Ausgabe wie Krüger und Stark. Für den Laptop enthält die DVD auch in diesem Fall das Werk als HTML, was bedeutet, dass es vom Komfort her keinen Unterschied gibt. Inhaltlich gehen die Autoren unterschiedlich vor. So widmet Ullenboom XML und JNI eigene Kapitel, während Krüger und Stark sich ausführlicher mit OOP-Aspekten auseinandersetzen. Ullenboom ist hier etwas aktueller, indem er das in Java SE 6 neue JAXB mit behandelt.

Thomas Stark hat, wie angedeutet, selbst einen Band zu Java veröffentlicht, den ebenfalls bei Addison-Wesley verlegten „Java EE 5“, der im Untertitel „Einstieg für Anspruchsvolle“ heißt. Den Unterschied zu den beiden Ungetümen sieht man schon am „EE“ (Enterprise Edition) im Titel sowie an der CD-ROM: JBoss und Tomcat sind dabei. Konsequenterweise dreht sich hier alles um Java Server Pages/Faces, Struts oder XML-Verarbeitung. Schmankerl für die Käufer des erstgenannten 1300-Seiters: Dessen DVD enthält dies Buch als PDF.

Wer keine Referenz benötigt und sich nicht mit einem Übermaß an Papier beschweren will, für den hat Addison-Wesley Berthold Daums „Java 6“ ins Programm aufgenommen. Anhand eines Dashboard-Projekts führt der Autor auf weniger als 500 Seiten ohne und mit GUI die Java-Programmierung vor – bis hin zu JAXB und Webservices. Weniger für Einsteiger als für diejenigen, die ihre Kenntnisse vertiefen wollen.



Agile Programmierung hängt grundsätzlich nicht von der verwendeten Sprache ab. Dennoch hat Michael Hüttermann sein gerade bei O’Reilly erschienenes Buch „Agile Java-Entwicklung“ zum großen Teil auf die eine Sprache beschränkt. Circa 120 Seiten stellen das Agile an sich dar, während die folgenden etwa 270 Seiten beschreiben, wie man die Methode mit Java-Werkzeugen wie Ant, JUnit, Maven und anderen umsetzt. Neulinge könnten sich überfordert fühlen.

Groovy ist *groovy* (toll, klasse) – und eine Skriptsprache für Java-Entwickler. In der Maiausgabe 2007 der *iX* war schon eine positive Besprechung des von Dierk König und anderen verfassten Manning-Buches „Groovy in Action“ zu lesen. Das hat den Hanser-Verlag nicht ruhen lassen, und noch im selben Jahr konnte Dorothea Heymann-Reders Übersetzung erscheinen. Am gründlichen Charakter der Einführung hat sich nichts geändert.

O’Reillys Alternative dazu ist Jörg Staudemeyers ebenfalls schon 2007 veröffentlichtes „Groovy für Java-Entwickler“. Vom Umfang her kaum mehr als die Hälfte des vorgenannten Bandes, kann dieser nicht dieselbe Ausführlichkeit bieten. Als Einstieg in die Java-Skriptsprache (als Implementierung des JSR 241) sollte er allemal hinreichen. Die Entscheidung zwischen den beiden Büchern fällt deshalb wahrscheinlich anhand der Anforderungen an die eigenen Anwendungen. Eine dritte Einführung veröffentlicht dieser Tage der dpunkt-Verlag.

Java ist nicht nur eine Insel; vor allem ist es Grundnahrungsmittel für Geeks, jene dem Klischee zufolge durcharbeitende Spezies, die sich mit Cola oder Kaffee und erkaltender Pizza wach hält, um beim agilen Programmieren nicht zu dösen. Mela Eckenfels und Petra Hildebrandt, beide nicht ungeekish, haben für diese Bevölkerungsgruppe in O’Reillys Kochbuch-Reihe endlich Ökotrophologisches (Haushalt und Ernährung) zusammengetragen. Von der Hardware (Küchenausrüstung) über diverse Links und eingestreute Rezepte bis zum UML-Diagramm für Muffins reicht das Spektrum. Locker geschriebener Geschenkkandidat.

Henning Behme

Joachim Baumann; Groovy; Grundlagen und fortgeschrittene Techniken; Heidelberg (dpunkt) 2008; 602 Seiten; € 46,– (gebunden)

Berthold Daum; Java 6; Programmieren mit der Java Standard Edition; München (Addison-Wesley) 2007; 475 Seiten; € 39,95 (gebunden)

Mela Eckenfels, Petra Hildebrandt; Das Kochbuch für Geeks; Köln (O’Reilly) 2007; 220 Seiten; € 15,90 (Paperback)

Michael Hüttermann; Agile Java-Entwicklung in der Praxis; Köln (O’Reilly) 2008; 397 Seiten; € 44,90 (gebunden)

Dierk König, Andrew Glover, Paul King, Guillaume Laforge, Jon Skeet; Groovy im Einsatz; übersetzt von Dorothea Heymann-Reder; München, Wien (Carl Hanser) 2007; 597 Seiten; € 49,90 (gebunden)

Guido Krüger, Thomas Stark; Handbuch der Java Programmierung; Standard Edition Version 6; München (Addison-Wesley) 2008; 1327 Seiten zzgl. DVD; € 49,95 (gebunden)

Thomas Stark; Java EE 5; Einstieg für Anspruchsvolle; München (Addison-Wesley) 2007; 534 Seiten zzgl. CD-ROM; € 29,95 (Paperback); als E-Buch € 32,–

Jörg Staudemeyer; Groovy für Java-Entwickler; Köln (O’Reilly) 2007; 330 Seiten; € 39,90 (Paperback)

Christian Ullenboom; Java ist auch eine Insel; Das umfassende Handbuch; Bonn (Galileo Computing) 2008; 7., aktualisierte und erweiterte Auflage; 1477 Seiten zzgl. DVD; € 49,90 (gebunden)



Thomas Künneth

Einstieg in Eclipse 3.3

Bonn 2007
Galileo Computing
394 Seiten
29,90 €
ISBN 978-3-89842-792-0

Eclipse als Platzhirsch der Java-IDEs füllt Heerscharen von Büchern. Der 3.3er Inkarnation hat sich Thomas Künneth mit einem reichhaltig bebildertem Werk genähert, das sich nicht lange mit der Theorie aufhält, sondern in dem der Leser gleich nach der Installation sein erstes Programm erstellt und die Grundlagen von Eclipse mitbekommt.

Künneth geht im Weiteren auf die Eigenheiten der IDE ein (Sichten, Editoren, Perspektiven). Einem ganzen Kapitel ist das Thema Arbeitsbereiche und Projekte gewidmet, wobei Tools wie Ant zur Sprache kommen. Da Eclipse von der Vielzahl der vorhandenen Plug-ins lebt, wird neben der Installation über den Update-Manager und dem technischen Verständnis für die Plug-in-Architektur gleich ein „Hello World“-Plug-in geschrieben. Es folgt eine kleine RCP-Anwendung. Debugging kommt ebenso zu seinem Recht (Breakpoints, bedingte Programmunterbrechung, Codeänderungen im Debug-Modus) wie die testgetrieben Entwicklung mit JUnit.

Auf CVS und Subversion geht Künneth mit dem nötigen Tiefgang ein (Einrichten eines Repositories, Konflikte managen, Arbeiten im Team). Ein Kapitel zum Erstellen einer GUI-Anwendung mit dem Editor Jigloo und eins zur Web- und Ajax-Programmierung runden den Band ab, dabei erläutert er Swing-Eigenheiten nur insoweit, wie sie zum Verständnis der Applikation notwendig sind. Im Web- und Ajax-Kapitel werden die Web Standard Tools als statische (HTML, CSS) und dynamische Projekte (J2EE Standard Tools als Bestandteil der Web Tools Platform) vorgestellt. Ebenso reißt Künneth das Google Web Toolkit, die Rich Ajax Platform und das Ajax Toolkit Framework an. Man kann kaum erwarten, dass ein Einstieg in Eclipse großen Tiefgang bei solch speziellen Abschnitten aufweist.

Obwohl Künneth auf die Eigenheiten der verschiedenen Betriebssysteme Windows, Linux und Mac OS X zu sprechen kommt, vergisst er gelegentlich eins. Dennoch ist sein Buch eins, das jedem ambitionierten Programmierer empfohlen werden kann. Java-Kenntnisse sollte der Leser mitbringen, da Künneth zwar einige Themen wie das Refactoring kurz anspricht, aber zu Recht gleich den Verweis auf Fowlers Klassiker anbringt.

KARSTEN KISSER



Georg Pietrek,
Jens Trompeter

Modellgetriebene Softwareentwicklung

MDA und MDSD in der Praxis

Frankfurt/Main 2007
Entwickler Press
256 Seiten
39,90 €
ISBN 978-3939084112

Modellgetriebene Softwareentwicklung ist eins der Trendthemen, dem sich wahrscheinlich kein Entwickler entziehen kann. Doch welche Vor- und Nachteile hat das MDSD (Model-Driven Software Development)? Wann lohnt sich sein Einsatz? Und welche Auswirkungen zeigen sich in Bezug auf die bestehenden Entwicklungsprozesse?

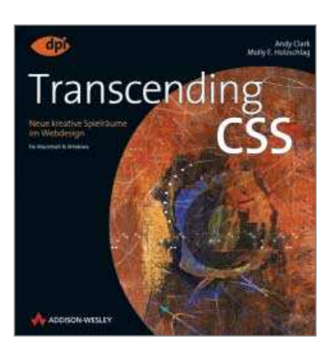
Diesen und einigen anderen Fragen gehen Pietrek und Trompeter zusammen mit einem großen Autorenteam auf den Grund. Zunächst sei vorweggenommen: Der Titel hält, was er verspricht, denn die Inhalte sind auf den Praxiseinsatz zugeschnitten. Damit richtet sich das Buch vor allem an IT-Manager, Projektleiter, Softwarearchitekten und Entwickler, die sich näher mit domänenspezifischen Sprachen und Modellierung auseinandersetzen und das Gelernte in eigenen Projekten umsetzen möchten.

In der Einleitung des gut strukturierten Bandes klären die Autoren, was man unter modellgetriebener Softwareentwicklung überhaupt versteht und welche Vorteile sie mit sich bringt. Jede Entwicklungsmethodik muss sich in bestehende Entwicklungsprozesse einfügen können. Dies ist Thema des nächsten Kapitels, das zeigt, wie sich MDSD in Kombination mit V-Modell XT, RUP und agilen Entwicklungsprozessen verhält. Im darauffolgenden Kapitel gehen die Autoren ausführlich darauf ein, wie man Softwaresysteme modellieren und validieren kann. Auf diese Erläuterungen folgen zahlreiche Erkenntnisse aus der Praxis. Den Einstieg bildet die Analyse zweier domänenspezifischer Sprachen und wie diese entworfen wurden.

Anschließend vermitteln Pietrek und Trompeter Best Practices für die MDSD. Sie erläutern die Verwendung von Codegeneratoren und stellen Strategien zur Versionierung der Quelltexte vor. Zudem erfährt man, wie MDSD in den Build-Prozess integriert werden kann und wie man solche Systeme dokumentiert. Der letzte Teil zeigt anhand eines durchgehenden Beispiels alle Schritte, die zur erfolgreichen Umsetzung einer einfachen Bibliothekssoftware nötig sind – beginnend bei der Erstellung des Anwendungsmodells bis hin zur fertigen Applikation.

Das Buch ist prägnant und kurzweilig zu lesen, die vielen Listings erlauben eine schnelle Umsetzung der gelernten Konzepte. Lediglich beim Code im letzten Kapitel fehlt ein wenig der Zusammenhang. Das stört allerdings kaum, da auf der CD-ROM eine Entwicklungsumgebung inklusive Listings zu finden ist. Damit können Leser sie sofort anpassen. Ein gutes Buch, das den Einstieg in die modellgetriebene Softwareentwicklung erfolgreich zu meistern hilft.

FLORIAN POTSCHKA



Andy Clarke,
Molly E. Holzschlag

Transcending CSS

Neue kreative Spielräume im Webdesign

München 2007
Addison-Wesley
Übersetzung: Jürgen Dubau
372 Seiten; 44,95 €
ISBN 978-3-8273-2545-7

Addison-Wesley hat sich in den letzten Jahren des Themas Webdesign mit CSS in einer Reihe von Büchern angenommen, darunter die von Eric Meyer und Jeffrey Zeldman. Mit dem vorliegenden ist eins hinzugekommen, das zu Recht neben den gerade genannten stehen darf. Eins gleich vorab: Das hier vorgestellte Buch ist nichts für CSS-Einsteiger. Es spricht vielmehr diejenigen an, die Erfahrungen mit XHTML sowie Cascading Stylesheets haben und größere Designschritte nach vorn beabsichtigen oder zumindest nicht ausschließen wollen. Was der britische Webdesigner Andy Clarke, der den Text zu verantworten hat, mit Unterstützung von Molly Holzschlag zustandegebracht hat, geht über Minimalanforderungen wie, dass alle Browser dasselbe zeigen sollen, weit hinaus.

Ausgehend von Webdesign-Entwicklungen der letzten Jahre beschreibt Clarke das sogenannte „progressive enhancement“ oder MOSe (Mozilla/Opera/Safari enhancement) und darauf aufbauend das den Buchtitel gebende Transcendent CSS. Verkürzt gesagt empfiehlt er: alle CSS-Selektoren nutzen, sogar die aus CSS3, keine Hacks und Filter, stattdessen notfalls Scripts verwenden. Ein solches Vorgehen bedeutet, dass standardkonforme Browser ein ausgeklügelteres Seitenlayout zeigen können als die, die CSS nicht so weit implementiert haben (beispielsweise Attributselektoren, mehrere Hintergrundbilder und Mehrspaltenlayout). Was dabei herauskommt, ist Design, das streng Inhalt von Präsentation trennt und immer wieder vom Motto „Die ganze Welt ist eine Liste“ (S. 79) ausgehend beschreibt, wie solches Simpel-Markup (*ul*, *ol*, *dl*) in elegant gestaltetes Design münden kann.

Üppig bebildert veranschaulicht der leicht querformatige Band oftmals, inwieweit das im Text Vorgetragene sich im Leben beziehungsweise dessen Ablichtung wiederfindet – beispielsweise die genannten Listen. Oder er betont Zitate, indem er sie eine ganze Seite einnehmen lässt.

Ob Namenskonventionen für „Standard“-*divs* oder Mikroformate, ob *z-index* oder Gitterdesign – quer durch das Werk finden sich Anregungen, die der Leser geneigt sein könnte, sofort ausprobieren zu wollen. Ein Rechner in Lesenähe bietet sich deshalb an.

Clarke ist sich nicht zu schade, immer wieder auf (Online-)Aufsätze anderer zu verweisen, was den Vorteil hat, dass mitschreibwütige Linksammler jede Menge spannender URLs sammeln können. Unter transcendingcss.com/support finden sich eine Reihe Listings zum Download, darunter leider nicht die URL-Sammlung.

Ein Buch, das Webdesigner, die nicht schon alles wissen, auf jeden Fall im Nachschlagezugriff haben sollten.

HENNING BEHME

Impressum



Postfach 61 04 07, 30604 Hannover; Helstorfer Straße 7, 30625 Hannover

Redaktion
Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de
Abonnements: Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Herausgeber: Christian Heise, Ansgar Heise

Redaktion: Chefredakteur: Jürgen Seeger (JS) -386

Stellv. Chefredakteur: Henning Behme (hb) -374

Ltd. Redakt.: Kersten Auel (ka) -367, Ralph Hülsenbusch (rh) -373, Bert Ungerer (un) -368

Jürgen Diercks (jd) -379, Christian Kirsch (ck) -590, Wolfgang Möhle (WM) -384, Susanne Nolte (sun) -689, André von Raison (avr) -377, Michael Riepe (mr) -787, Ute Roos (ur) -535

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

Korrespondent Köln/Düsseldorf/Ruhrgebiet:
Achim Born, Siebengebirgsallee 82, 50939 Köln,Telefon: 02 21/4 20 02 62,
E-Mail: ab@ix.de

Korrespondentin München:
Susanne Franke, Ansbacherstr. 2, 80796 München, Telefon: 089/28 80 74 80,
E-Mail: sf@ix.de

Ständige Mitarbeiter: Torsten Beyer, Detlef Borchers, Fred Hantelmann, Kai König, Michael Kuschke, Barbara Lange, Stefan Mintert, Holger Schwichtenberg, Susanne Schwonbeck, Christian Segor, Diane Sieger, Axel Wilzopolski, Nikolai Zotow

DTP-Produktion: Enrico Eisert, Wiebke Preuß, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat/Chefin vom Dienst: Anja Fischer

Fotografie: Martin Klauss Fotografie, Despetal/Barfelde

Titelidee: ***iX;*** Titel- und Aufmachergestaltung: Dietmar Jokisch

Verlag und Anzeigenverwaltung:
Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Helstorfer Straße 7, 30625 Hannover; Telefon: 05 11/53 52-0, Fax: 05 11/53 52-129

Geschäftsführer: Ansgar Heise, Steven P. Steinkraus, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de

Assistenz: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigendisposition: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigenverkauf: PLZ-Gebiete 0–3, Ausland:
Oliver Kühn -395, E-Mail: oliver.kuehn@heise.de,
PLZ-Gebiete 8–9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de
Sonderprojekte: Isabelle Paeseler -205, E-Mail: isabelle.paeseler@heise.de

Anzeigen-Inlandsvertretung: PLZ-Gebiete 4–7:
Karl-Heinz Kremer GmbH, Sonnenstraße 2, D-66957 Hilst,
Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22, E-Mail: karlheinz.kremer@heise.de

Anzeigen-Auslandsvertretung:
Großbritannien, Irland: Oliver Smith & Partners Ltd. Colin Smith, 18 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX, UK, Telefon: (00 44) 20/79 78-14 40, Fax: (00 44) 20/79 78-15 50,
E-Mail: colin@osp-uk.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 20 vom 1. Januar 2008.

Leiter Vertrieb und Marketing: Mark A. Cano (-299)

Werbeleitung: Julia Conrades (-156)

Teamleitung Herstellung: Bianca Nagel (-456)

Druck: Dierichs Druck + Media GmbH & Co. KG, Kassel

Sonderdruck-Service: Ruth Utesch (-359, Fax: -360)

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

***iX* erscheint monatlich**

Einzelpreis € 5,50, Österreich € 6,20, Schweiz CHF 10,70, Benelux € 6,70, Italien € 6,70

Das Abonnement für 12 Ausgaben kostet: Inland € 56,–, Ausland (außer Schweiz) € 63,–; Studentenabonnement: Inland € 42,–, Ausland (außer Schweiz) € 47,– nur gegen Vorlage der Studienbescheinigung (inkl. Versandkosten Inland € 8,30, Ausland € 13,30), Luftpost auf Anfrage.

iX-Abo+ (inkl. jährlicher Archiv-CD-ROM) jeweils zzgl. € 8,–

Für GI-, VDI-KfIT-, GUUG-, IUG-, LUG-, AUGE- und Mac-e.V.-Mitglieder gilt der Preis des Studentenabonnements (gegen Mitgliedsausweis).

Kundenkonto in Österreich:
Dresdner Bank AG, BLZ 19675, Kto.-Nr. 2001-226-00 EUR, SWIFT: DRES AT WX

Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0

Abo-Service:
Heise Zeitschriften Verlag, Kundenservice, Postfach 810520, 70522 Stuttgart,
Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Für Abonnenten in der Schweiz Bestellung über:
Thali AG, Aboservice, Industriestr. 14, CH-6285 Hitzkirch,
Telefon: 041/919 66 11, Fax: 041/919 66 77, E-Mail: abo@thali.ch, Internet: www.thali.ch (Jahresabonnement: CHF 111,–; Studentenabonnement: CHF 83,25)

Das Abonnement ohne Archiv-CD-ROM ist jederzeit mit Wirkung zur jeweils übernächsten Ausgabe kündbar. Das *iX-Abo+* (incl. jährlicher Archiv-CD-ROM) gilt zunächst für ein Jahr und ist danach zur jeweils übernächsten Ausgabe kündbar.

Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz): MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Str. 5, 85386 Eching, Telefon: 089/319 06-0,
Fax: 089/319 06-113, E-Mail: mzv@mzv.de, Internet: www.mzv.de



ISSN 0935-9680



Open-Source-Business-Modelle

Würde ein Händler seine Waren verschenken, anstatt sie gewinnbringend an den Mann oder die Frau zu bringen, wäre er innerhalb kürzester Zeit pleite. Doch in der Software-Industrie beginnt sich mit dem Erfolg von Open Source ein Geschäftsmodell zu etablieren, das genau dies zum Prinzip erhebt – das überwiegende Verschenken der eigenen Produkte. *iX* erklärt, warum das trotzdem funktionieren kann.

ECM als Open Source

Produkte, die Enterprise Content Management (ECM) versprechen, kommen üblicherweise für teures Geld ins Haus. Mit Alfresco existiert immerhin ein solches System, das als Open Source keinen initialen Kostendruck erzeugt. Es nutzt eine Reihe von Java-Werkzeugen – Tomcat, Hibernate, Spring et cetera – und besteht aus einem Datenbank-Backend, einem Application Server sowie dem Browser als Frontend. Versionsstand ist 2.1, verfügbar ist das ECMS für Windows und Linux.

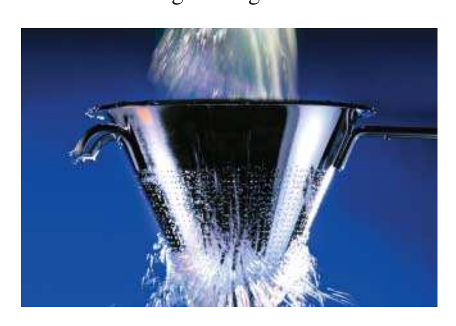
Heft 06/2008 erscheint am 15. Mai 2008

Mailserver als Fertigprodukt

Zu den letzten großen Geheimnissen des Internet scheint das störungsfreie Betreiben von Mailservern zu gehören. Daher greifen viele Anwender gerne zu Komplettpaketen aus Soft- und Hardware, sogenannten Appliances – in der Hoffnung, dass darin auch kompetente Entwicklungsarbeit steckt. Ein Überblick über den im Bereich E-Mail besonders vielfältigen Appliance-Markt.

Sicherheitstests per Google

Wenn es um das Aufspüren verwundbarer Webseiten oder das Sammeln vertraulicher Informationen geht, ist Google-Hacking seit einiger Zeit das Mittel der Wahl. Es war nur eine Frage der Zeit, bis jemand auf die Idee kam, diese Technik zu automatisieren und mit einer bequemen Benutzeroberfläche zu versehen. Ein Test zeigt, wie effektiv das Hackerwerkzeug Goolag wirklich ist.



VoIP-Sicherheit versus Sprachverständlichkeit

Wer mit Voice over IP sicher telefonieren will, kommt um zusätzliche Maßnahmen wie VPN-Tunnel nicht herum. Das Verschlüsseln kostet jedoch Rechenzeit und führt zu Verzögerungen beim IP-Paketversand. Wie sich das auf die Sprachqualität auswirkt, berichtet *iX* in der nächsten Ausgabe.